



Universidad
Carlos III de Madrid

- PROYECTO FIN DE CARRERA -

ESTUDIO E IMPLANTACIÓN DE UNA RED CABLEADA, WIFI Y SEGURIDAD EN UN CENTRO EDUCATIVO

Autor: Diego Durán Fernández

Tutor: Anabel Fraga Vázquez

Leganés, Octubre 2015

Título: Estudio e implantación de una red cableada, wifi y seguridad en un centro educativo.

Autor: Diego Durán Fernández

Director: Anabel Fraga Vázquez

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día ___ de Octubre de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO

PRESIDENTE

DEDICATORIA Y AGRADECIMIENTOS

Uno empieza el camino con grandes expectativas y con unas ganas tremendas de comerse el mundo, el tiempo pasa y pone las cosas en su sitio.

Siempre pensé que cuando uno empieza algo no debe dejarlo a medias, ha de terminarlo, en mi caso casi no lo terminé y por eso hoy valoro más que nunca el poder tener algo con lo que soñé desde que era pequeño.

En mi familia siempre se tuvieron grandes expectativas sobre mí y a día de hoy me doy cuenta que he terminado este camino no por lo que los demás esperen de mí y si por el respeto que me tengo a mi mismo y por demostrarme que con trabajo todo se logra.

En este camino he de agradecer el apoyo de muchas personas que nunca dejaron de creer en mí...

A mis padres Diego y Francisca, que lo han dado todo para que yo pueda tener el futuro mejor, y a pesar de los disgustos que he podido darles, su orgullo el día de hoy hacia mí me llena de alegría.

A mi hermano David, que gracias a su ayuda sobre todo económica durante los años de universidad permitieron que este sueño se haga realidad.

A mis “pájaros”, especial mención a Jose del Castillo (los hermanos a veces no se encuentran en tu familia), que empezaron el camino a mi lado e increíblemente siguen ahí, ellos han sido mi motivación y mi apoyo todos y cada uno de los días en la universidad.

A mi tutora Anabel Fraga, fue capaz de dar la oportunidad de terminar la carrera a un alumno que le quedaba poquísimo para poder realizar este proyecto. Gracias de verdad, ya casi lo daba por perdido.

A todos los profesores que han pasado por mi vida académica porque ellos me han empujado hasta terminar este camino, tanto los buenos como los malos.

A Roberto López, no puedo llamarle amigo, ni hermano, ha trascendido toda clasificación en mi vida, le admiro en todas y cada una de las facetas de la

vida, ejemplo de superación e influencia en mi vida a niveles que no puedo definir.

A Sara Garcia Moreno, mi pareja, una persona que ha logrado que siga persiguiendo todos mis sueños, ejemplo de superación, determinación y de lucha en la vida, nos queda toda una vida juntos y muchos proyectos que empezar y terminar.

Para finalizar este apartado, he de agradecer a todos esos amigos que no he nombrado, personas que de alguna manera han logrado influirme y empujarme a avanzar en la vida, de los que he intentado absorber todo lo bueno que tienen para que me hicieran mejor persona.

INDICE GENERAL

1. Introducción.....	13
2. Objetivos.....	14
3. Requerimientos.....	15
4. Estado del Arte.....	16
4.1 Tipos de Redes.....	16
4.2 Arquitectura de Redes.....	17
4.2.1 Introducción.....	17
4.2.2 Características.....	17
4.2.3 Tipos.....	18
4.2.3.1 SRA.....	18
4.2.3.2 Arquitectura de red digital (DRA).....	19
4.2.3.3 ARCnet.....	20
4.2.3.4 Ethernet.....	21
4.2.3.4.1 Funciones.....	22
4.2.3.4.2 Formato de trama.....	23
4.3 Modelo OSI.....	25
4.3.1 Funciones de los niveles.....	26
4.4 Arquitectura TCP/IP.....	29
4.4.1 Características.....	29
4.4.2 Funciones de los niveles TCP/IP.....	30
4.5 Hardware.....	31
4.5.1 Cables.....	31
4.5.1.1 Tipos de Cables.....	32
4.5.1.1.1 Coaxial.....	32
4.5.1.1.2 Par trenzado.....	34
4.5.1.1.3 Fibra óptica.....	36
4.5.1.1.3.1 Características.....	37
4.5.1.1.3.2 Tipos.....	37
4.5.2 Dispositivos de red.....	38
4.5.2.1 Hubs.....	38
4.5.2.2 Switches.....	39
4.5.2.3 Routers (enrutador).....	40

4.5.2.3.1 Tipos de enrutamiento.....	42
4.5.2.3.1.1 Enrutamiento estático.....	42
4.5.2.3.1.2 Enrutamiento dinámico.....	43
4.5.2.4 Puntos de acceso (Wireless Access Point).....	43
4.6 LAN WIFI.....	45
4.6.1 Estándares WIFI.....	46
4.6.1.1 IEEE 802.11.....	46
4.6.1.1.1 802.11a.....	46
4.6.1.1.2 802.11b.....	46
4.6.1.1.3 802.11g.....	47
4.6.1.1.4 802.11n.....	48
4.7 Seguridad.....	49
4.7.1 Protocolos de cifrado.....	49
4.7.1.1 WEP.....	50
4.7.1.2. WPA.....	50
4.7.1.3. WPA2.....	51
4.7.1.4. IPsec.....	52
4.7.1.5. DES.....	52
4.7.1.6. AES.....	55
5. Diseño de la red.....	58
5.1 Descripción del entorno.....	58
5.2 Distribución de los elementos de la red.....	60
5.3 Direccionamiento lógico de la red.....	65
5.4 Elección del cableado y velocidad de la red.....	66
5.5 Elección y configuración de la electrónica de red.....	67
5.5.1 Switches y su configuración.....	67
5.5.2 Puntos de Acceso.....	70
5.5.3 Modem-Router de salida a internet.....	73
5.6 Otros elementos de apoyo docente.....	74
5.6.1 Equipos y Software básico.....	74
5.6.2 Impresoras.....	81
5.6.3 Pizarras digitales y proyectores.....	83

6. Presupuesto.....	86
7. Posibles mejoras y perspectivas de futuro.....	90
8. Bibliografía.....	92
9. Glosario.....	93
10. Anexos.....	96
10.1 Anexo A – Planos del edificio.....	96
10.2 Anexo B - Diagramas De Red.....	99

INDICE DE FIGURAS Y PLANOS

Figura 1. Formato Trama Ethernet.....	23
Figura 2. Modelo OSI.....	25
Figura 3. Encapsulamiento de la trama.....	28
Figura 4. Modelo TCP/IP.....	29
Figura 5. Comparación OSI Vs. TCP/IP.....	31
Figura 6. Cable Coaxial.....	33
Figura 7. Cable de par trenzado UTP.....	34
Figura 8. Cable de par trenzado STP.....	35
Figura 9. Cable de par trenzado FTP.....	36
Figura 10. Cable de Fibra Óptica.....	37
Figura 11. Tipos de cable de Fibra Óptica.....	38
Figura 12. Hubs.....	39
Figura 13. Switch.....	40
Figura 14. Routers.....	42
Figura 15. Punto de Acceso.....	44
Figura 16. Cálculo de subclaves, Ki.....	53
Figura 17. Ronda del algoritmo DES.....	54
Figura 18. Etapa SubBytes.....	56
Figura 19. Etapa ShiftRows.....	56
Figura 20. Etapa MixColumns.....	56
Figura 21. Etapa AddRoundKey.....	57
Figura 22. Armario mural de 19" con doble cuerpo y llave.....	61

Figura 23. Ventilador para refrigeración superior del rack (No ocupa unidad)..	63
Figura 24. D-Link DES-1210-52.....	69
Figura 25. AP Cisco MR32.....	71
Figura 26. Enlace WDS con admisión de clientes.....	71
Figura 27. Modem- Router WRT1900ACS.....	74
Figura 28. Pantalla de elección de unidades congeladas durante la instalación de Deep Freeze.....	77
Figura 29. Barra de tareas, icono de estado de Deep Freeze.....	77
Figura 30. Ventana de introducción de password en Deep Freeze.....	78
Figura 31. Panel de control de Deep Freeze.....	79
Figura 32. PDI.....	84
Figura 33. Capacidad de instalación del proyector de corto alcance.....	85
Figura 34. Planta 0 Infantil.....	96
Figura 35. Planta 1 Primaria.....	97
Figura 36. Planta 2 ESO.....	98
Figura 37. Distribución general de la red.....	99

INDICE DE TABLAS

Tabla 1. Comparativa categorías cable par trenzado.....	35
Tabla 2. Comparación estándares 802.11.....	46
Tabla 3. Desglose de puntos de red.....	58
Tabla 4. Desglose del reparto de electrónica de red en los armarios.....	61
Tabla 5. Representación del Rack.....	64
Tabla 6. Características básicas del Switch D-1210-52.....	70
Tabla 7. Características AP MR34 de Cisco.....	72
Tabla 8. Datos que deben cumplir los equipos miembros de una red WDS.....	73
Tabla 9. Características Modem-Router WRT1900ACS.....	74
Tabla 10. Aplicaciones a instalar en los PC`s del centro.....	76
Tabla 11. Desglose de equipos a instalar.....	81
Tabla 12. Desglose de impresoras a instalar.....	82
Tabla 13. Características impresoras.....	83
Tabla 14. Presupuesto electrónica de red.....	87
Tabla 15. Presupuesto equipamiento informático.....	89

1. Introducción y justificación del proyecto

Este proyecto nace por la necesidad de modernizar las instalaciones de un centro escolar, adecuándolas a los tiempos en los que estamos y proporcionar una conectividad a diferentes dispositivos con el objetivo de facilitar la enseñanza a los alumnos y darles la facilidad a los profesores de tener acceso a todo el material didáctico de una forma rápida y sencilla.

En la historia de la informática, la velocidad en la innovación de las tecnologías es imparable y evidentemente esta misma evolución ha de llegar a los centros de educación, atrás deben quedar los métodos en los que los alumnos utilizaban un ordenador una hora en la semana y con suerte, dichos alumnos a día de hoy han de saber no solo manejar la tecnología sino que además han de aprovecharla para sacar el máximo rendimiento a los materiales didácticos que se les pueda proporcionar. Igualmente el colectivo del profesorado ha de poder tener acceso y poder proporcionar una educación acorde a los tiempos que corren con los medios tecnológicos más adecuados, enseñando a los alumnos que un ordenador no solo sirve para jugar y divertirse (chatear, redes sociales...), sino para desarrollar una serie de capacidades y conocimiento que posteriormente les va a servir para su vida tanto personal como profesional.

En este caso vamos a estudiar la posibilidad de implantar una red tanto cableada como inalámbrica en un centro de estudios, se estudiará y evaluarán las necesidades del centro y se propondrán soluciones a dichas necesidades tanto en HW como en SW. También se estudiará que tecnología es la más adecuada y la securización de dicha red.

Una vez expuestas, analizadas y justificadas las decisiones técnicas y óptimas para el centro y estudiadas las alternativas, se realizará un estudio económico de realización del proyecto.

2. Objetivos

Partiendo de los conceptos ya introducidos, vamos a proporcionar a un centro educativo con una red informática, tanto cableada como inalámbrica, que contenga una dotación tecnológica razonable para dicho centro y que ayude al profesor y al alumno a aprovechar todos y cada uno de los recursos tecnológicos del centro.

Diseñar la red tanto cableada como Wireless de manera que haya cobertura sin problema en todo el centro de manera que pueda ser aprovechada por el mayor número de dispositivos posible.

Utilizar los equipos adecuados para dar mayor funcionalidad y rendimiento al sistema.

Realizar un cálculo de costes del proyecto.

La metodología a seguir contará con un análisis del centro educativo, donde debemos conocer las características del mismo y además las zonas necesarias con cobertura.

La metodología se puede dividir en las siguientes fases:

- Planificación.
- Diseño.
- Implantación.
- Puesta en marcha.

No hay que descuidar temas como los relacionados con aspectos legales y de seguridad. En esta memoria, se podrán estudiar con más detalle.

3. Requerimientos

El proyecto se desarrolla en un centro educativo de infantil y primaria. Habrá por lo tanto dos tipos de usuarios bien diferenciados de la red. Por un lado el personal docente que utilizara los sistemas disponibles para preparar e impartir las clases, y por otro lado los alumnos, que utilizaran el material técnico como herramienta para ampliar sus conocimientos o acceder a parcelas de conocimiento diferentes al clásico libro de texto.

Será necesario un esfuerzo especial por parte de los docentes para estar mínimamente formados y al día sobre las nuevas tecnologías y saber manejar con cierta soltura las herramientas de que dispondrán.

No existirá ningún servidor centralizado ni aplicaciones en red, por lo que cada equipo usará la red básicamente para imprimir en las impresoras compartidas disponibles y como vehículo para salir a Internet, por lo tanto la seguridad no será un punto vital. Excepcionalmente se podrá pasar información de un equipo a otro, pero no es el servicio principal del sistema a implantar.

En cualquier caso, el proyecto prevé la implantación de un sistema flexible, escalable y ampliable con modificaciones de forma escalonada a lo largo del tiempo según las necesidades futuras del centro, dejando la puerta abierta para instalar nuevos sistemas y dar cobertura a futuras tecnologías que trabajen sobre la red local a implantar.

4. Estado del arte

Para poder realizar este proyecto, tenemos que entender que es una red y conocer cuáles son las partes más importantes que actúan en la misma y cuál es su función.

En nuestro proyecto se usaran los dispositivos que sean necesarios para el desarrollo, implantación y uso de la misma.

4.1 Tipos de redes

Según extensión: Estas redes se pueden diferenciar según el área geográfica que abarcan, pudiéndose clasificar en:

- PAN (Personal Area Network): Redes de área personal, la distancia entre los ordenadores no es mayor a 1 metro.
- LAN (Local Area Network): Redes de área local, la distancia entre los ordenadores ya puede ser mayor, normalmente no superiores a 1 Km., como por ej. redes que hay en edificios, campus, o aulas.
- MAN (Metropolitan Area Network): Redes de área metropolitana, son aquellas que unen ordenadores situados en una extensión parecida a una ciudad, la distancia no suele superar los 10 Km.
- WAN (Wide Area Network): Redes de área amplia, estas redes unen ciudades, países, continentes, como ejemplo sería Internet.

Según la direccionalidad de los datos:

- Simplex (unidireccionales): Los datos solo circulan en una dirección. EJ.: las antenas parabólicas normales, que solo reciben señal.
- Half-duplex (bidireccionales): los datos pueden circular en ambas direcciones, pero solo una a la vez, es decir, si alguien envía datos, no van a poder emitir más datos hasta que estos lleguen a su destino, ni podrá recibir a la vez.
- Full-duplex (bidireccional total): los datos pueden ser enviados y recibidos a la vez, tanto el emisor como el receptor pueden enviar y recibir al mismo tiempo.

4.2 Arquitectura de redes

4.2.1 Introducción

Es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto coordinado de productos que se puedan interconectar. La arquitectura es el “plan” con el que se conectan los protocolos y otros programas de software. Esto es benéfico tanto para los usuarios de la red como para los proveedores de hardware y software.

4.2.2 Características

Separación de funciones: dado que la arquitectura separa los usuarios y los productos evolucionan con el tiempo, las nuevas funcionalidades han de adaptarse de manera fácil a las anteriores, por este motivo las arquitecturas tienen un alto grado de modularidad, de esta manera los cambios que se van dando afectan lo menos posible.

Amplia conectividad: El objetivo de dichas arquitecturas es proporcionar la mayor cobertura entre los nodos que existan teniendo en cuenta la seguridad necesaria.

Recursos compartidos: Hace que la operación de red sea más efectiva y económica ya que permite compartir BBDD, impresoras...

Administración de la red: dentro de la arquitectura se ha de permitir que el usuario defina, opere, cambie, proteja y dé mantenimiento a la red.

Facilidades de uso: permite que los diseñadores se centren en las interfaces primarias y de esta manera hacerlas más amigables para el usuario.

Normalización: con la arquitectura se favorece que todo esté normalizado tanto SW como HW y de esta manera se ahorran costes.

Administración de datos: En la arquitectura de red se tiene en cuenta la necesidad de interconectar todos los sistemas de admón. de BBDD.

Interfaces: En las arquitecturas se definen las interfaces de persona a red, de persona a programa y de programa a programa, así se utilizan los protocolos adecuados y paquete SW para hacer una red funcional.

Aplicaciones: En las arquitecturas de red se separan las funciones de operar una red a partir de las aplicaciones comerciales de la organización, para tener más eficiencia cuando los programadores del negocio no necesitan considerar la operación.

4.2.3 Tipos

4.2.3.1 SRA

(Distribuida por IBM) Con la ASR se describe una estructura integral que provee todos los modos de comunicación de datos y con base en la cual se pueden planear e implementar nuevas redes de comunicación de datos.

La ASR se construyó en torno a cuatro principios básicos:

- Comprende las funciones distribuidas con base en las cuales muchas responsabilidades de la red se puede mover de la computadora central a otros componentes de la red como son los concentradores remotos.
- Define trayectorias ante los usuarios finales (programas, dispositivos u operadores) de la red de comunicación de datos en forma separada de los usuarios mismos, lo cual permite hacer extensiones o modificaciones a la configuración de la red sin afectar al usuario final.
- Se utiliza el principio de la independencia de dispositivo, lo cual permite la comunicación de un programa con un dispositivo de entrada / salida sin importar los requerimientos de cualquier dispositivo único. Esto también permite añadir o modificar programas de aplicación y equipo de comunicación sin afectar a otros elementos de la red de comunicación.
- Se utilizan funciones y protocolos lógicos y físicos normalizados para la comunicación de información entre dos puntos cualesquiera, y esto significa que se puede tener una arquitectura de propósito general y terminales de muchas variedades y un solo protocolo de red.

La organización lógica de una red ASR, se divide en dos grandes categorías de componentes:

- Unidades direccionales de red: son grupos de componentes de ASR que proporcionan los servicios mediante los cuales el usuario final puede enviar datos a través de la red y ayudan a los operadores de la red a realizar el control de esta y las funciones de administración.
- Red de control de trayectoria: provee el control de enrutamiento y flujo; el principal servicio que proporciona la capa de control del enlace de datos dentro de la red de control de trayectoria es la transmisión de datos por enlaces individuales. Tiene dos capas:
 - La capa de control de trayectoria: Los principales servicios proporcionados son el control de enrutamiento y de flujo.
 - la capa de control de enlace de datos: el principal servicio que proporciona es la transmisión de datos por enlaces individuales.

4.2.3.2 Arquitectura de red digital (DRA)

Esta es una arquitectura de red distribuida de la Digital Equipment Corporation. Se le llama DECnet y consta de cinco capas. La capa física, de control de enlace de datos, de transporte y de servicios de la red corresponden casi exactamente a las cuatro capas inferiores del modelo OSI. La quinta capa, la de aplicación, es una mezcla de las capas de presentación y aplicación del modelo OSI. La DECnet no cuenta con una capa de sesión separada.

La DECnet define un marco general tanto para la red de comunicación de datos como para el procesamiento distribuido de datos. El objetivo de la DECnet es permitir la interconexión generalizada de diferentes computadoras principales y redes punto a punto, multipunto o conmutadas de manera tal que los usuarios puedan compartir programas, archivos de datos y dispositivos de terminal remotos.

La DECnet soporta la norma del protocolo internacional X.25 y cuenta con capacidades para conmutación de paquetes. Se ofrece un emulador mediante el cual los sistemas de la Digital Equipment Corporation se pueden interconectar con las macrocomputadoras de IBM y correr en un ambiente

ASR. El protocolo de mensaje para comunicación digital de datos (PMCD) de la DECnet es un protocolo orientado a los bytes cuya estructura es similar a la del protocolo de Comunicación Binaria Síncrona (CBS) de IBM.

4.2.3.3 ARCnet

La Red de computación de recursos conectadas (ARCNET, Attached Resource Computing Network) es un sistema de red banda base, con paso de testigo (token) que ofrece topologías flexibles en estrella y bus a un precio bajo. Las velocidades de transmisión son de 2.5 Mbits/seg. ARCNET usa un protocolo de paso de testigo en una topología de red en bus con testigo, pero ARCNET en sí misma no es una norma IEEE. En 1977, Datapoint desarrollo ARCNET y autorizo a otras compañías. En 1981, Standard Microsystems Corporation (SMC) desarrollo el primer controlador LAN en un solo chip basado en el protocolo de paso de testigo de ARCNET. En 1986 se introdujo una nueva tecnología de configuración de chip.

ARCNET tiene un bajo rendimiento, soporta longitudes de cables de hasta 2000 pies cuando se usan concentradores activos. Es adecuada para entornos de oficina que usan aplicaciones basadas en texto y donde los usuarios no acceden frecuentemente al servidor de archivos. Las versiones más nuevas de ARCNET soportan cable de fibra óptica y de par-trenzado. Debido a que su esquema de cableado flexible permite de conexión largas y como se pueden tener configuraciones en estrella en la misma red de área local. ARCNET es una buena elección cuando la velocidad no es un factor determinante pero el precio sí.

Proporciona una red robusta que no es tan susceptible a fallos como Ethernet de cable coaxial si el cable se suelta o se desconecta. Esto se debe particularmente a su topología y a su baja velocidad de transferencia. Si el cable que une una estación de trabajo a un concentrador se desconecta o corta, solo dicha estación de trabajo se va a abajo, no la red entera. El protocolo de paso de testigo requiere que cada transacción sea reconocida, de modo no hay cambios virtuales de errores, aunque el rendimiento es mucho más bajo que en otros esquemas de conexión de red.

4.2.3.4 Ethernet

Desarrollado por la compañía XERTOX y adoptado por la DEC (Digital Equipment Corporation), y la Intel, Ethernet fue uno de los primeros estándares de bajo nivel. Actualmente es el estándar más ampliamente usado.

Ethernet está principalmente orientado para automatización de oficinas, procesamiento de datos distribuido, y acceso de terminal que requieran de una conexión económica a un medio de comunicación local transportando tráfico a altas velocidades.

Este protocolo está basado sobre una topología bus de cable coaxial, usando CSMA/CD ("Acceso Múltiple por Detección de Portadora con Detección de Colisiones") para acceso al medio y transmisión en banda base a 10 MBPS. Además de cable coaxial soporta pares trenzados. También es posible usar Fibra Óptica haciendo uso de los adaptadores correspondientes.

Además de especificar el tipo de datos que pueden incluirse en un paquete y el tipo de cable que se puede usar para enviar esta información, el comité especificó también la máxima longitud de un solo cable (500 metros) y las normas en que podrían usarse repetidores para reforzar la señal en toda la red. Con este tipo de redes, se podrá intercambiar información entre computadoras y manejar completamente una computadora desde la otra. Además se podrá compartir el acceso a internet.

Las especificaciones de Ethernet describen como los datos pueden ser enviados entre computadoras en una proximidad física en lo que es llamado red de área local: LAN. Para ser una parte de ésta LAN, cada computadora necesita una interface de red (que "empaqueta" los datos para que "viajen" a través de la red) y un punto de conexión, o puerto, para el cableado especial que conecta todas las PC's.

La forma de enviar datos es segura, ya que emplea un protocolo especial para Ethernet llamado Acceso Múltiple por Detección de Portadora con Detección de Colisiones (CSMA/CD). La información se envía en forma de paquetes, y es muy seguro, ya que si se pierde alguno, se vuelven a enviar.

En estas redes, las computadoras están conectadas a un hub, que es un dispositivo central que se encarga de distribuir de forma correcta los paquetes de información.

Además de esta, existen otras formas de enviar la información, todo depende de la cantidad de computadoras que desees conectar. Si solo desees conectar dos, la red es peer-to-peer, que se instala de forma sencilla y va desde un puerto al otro de las computadoras.

Las conexiones Ethernet pasan información rápidamente. Por ejemplo el 10 Base-T, pasa 10 megabits por segundo; aunque con la mejoría de las redes en el cableado, la información que pasa actualmente es varias veces mayor.

En la actualidad se está implementando una nueva tecnología llamada Ethernet 10-gbps, que envía 10 gigabits por segundo.

Como vemos, disponemos de muy buenas velocidades para conectarse en red, además es bastante accesible. De esta forma podrás compartir con las máquinas una sola conexión a internet y además no será necesario que cambies los periféricos de lugar, ya que puedes usarlos remotamente.

4.2.3.4.1 Funciones

Encapsulación de datos:

- Formación de la trama estableciendo la delimitación correspondiente.
- Direccionamiento del nodo fuente y destino.
- Detección de errores en el canal de transmisión.

Manejo de Enlace:

- Asignación de canal.
- Resolución de contención, manejando colisiones.

Codificación de los Datos

- Generación y extracción del preámbulo para fines de sincronización.
- Codificación y decodificación de bits.

Acceso al Canal:

- Transmisión / Recepción de los bits codificados.
- Sensibilidad de portadora, indicando tráfico sobre el canal.
- Detección de colisiones, indicando contención sobre el canal.

4.2.3.4.2 Formato de trama

En una red ethernet cada elemento del sistema tiene una dirección única de 48 bits, y la información es transmitida serialmente en grupos de bits denominados tramas. Las tramas incluyen los datos a ser enviados, la dirección de la estación que debe recibirlos y la dirección de la estación que los transmite.

Cada interface ethernet monitorea el medio de transmisión antes de una transmisión para asegurar que no esté en uso y durante la transmisión para detectar cualquier interferencia.

En caso de alguna interferencia durante la transmisión, las tramas son enviadas nuevamente cuando el medio esté disponible. Para recibir los datos, cada estación reconoce su propia dirección y acepta las tramas con esa dirección mientras ignora las demás.

El tamaño de trama permitido sin incluir el preámbulo puede ser desde 64 a 1518 octetos. Las tramas fuera de este rango son consideradas inválidas.

7 B	1 B	6 B	6 B	2 B	0-1500 B	0-46 B	4 B
Preámbulo	S O F	Dir. Destino	Dir. Fuente	Tipo	Datos	Relleno	CRC
a)							
8 B	6 B		6 B	2 B	0-1500 B	0-46 B	4 B
Preámbulo	Dir. Destino		Dir. Fuente	Largo	Datos	Relleno	CRC
b)							

Figura 1. Formato Trama Ethernet

- Preámbulo: Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de Trama (SOF) de la trama IEEE 802.3.
- Inicio de trama (SOF): Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.
- Direcciones destino y origen: Incluye las direcciones físicas (MAC) únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección única, mientras que la de destino puede ser de broadcast única (trama enviada a una sola máquina), de broadcast múltiple (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).
- Tipo (Ethernet): Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.
- Longitud (IEEE 802.3): Indica la cantidad de bytes de datos que sigue este campo.
- Datos: Incluye los datos enviados en la trama. En las especificación IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama). Por su parte, las especificaciones Ethernet versión 2 no especifican ningún relleno, Ethernet espera por lo menos 46 bytes de datos.
- Secuencia de verificación de trama (FCS): Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el checksum de verificación de la trama, comprueba que los datos corresponden a un mensaje IP y entonces lo pasa a dicho protocolo para que lo procese. El tamaño máximo de los paquetes en las redes Ethernet es de 1500 bytes.

4.3 Modelo OSI

El modelo OSI surge como una búsqueda de solución al problema de incompatibilidad de las redes de los años 60. Fue desarrollado por la ISO (International Organization for Standardization) en 1977 y adoptado por UIT-T.

Consiste de una serie de niveles que contienen las normas funcionales que cada nodo debe seguir en la Red para el intercambio de información y la interoperabilidad de los sistemas. Cada nivel del OSI es un módulo independiente que provee un servicio para el nivel superior dentro de la Arquitectura o modelo.

El objetivo del Modelo OSI es formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema independientemente del fabricante, arquitectura, localización, SO...



Figura 2. Modelo OSI

En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora está enviándole información. Cualquier nivel dado, puede incorporar un encabezado

al mensaje. Por esta razón, se considera que un mensaje está constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

Cada capa de la arquitectura realiza una función bien definida.

Cada nivel interacciona con los niveles inmediatos superior e inferior.

4.3.1 Funciones de los niveles

Físico: Es el nivel encargado del control del transporte físico de la información entre dos puntos. Define características funcionales tales como:

- Establecer, mantener y liberar las conexiones punto a punto y multipunto.
- Tipo de transmisión asincrónica o sincronía.
- Modo de operación simplex, half-duplex, full-dúplex.
- Velocidad de transmisión.
- Niveles de voltaje.
- Distribución de pines en el conector y sus dimensiones.
- En este nivel se definen las interfaces, módem, equipos terminales de línea, etc.

Enlace:

- Detecta y corrige todos los errores que se produzcan en las líneas de comunicación
- Controla que un emisor rápido no sature a un receptor lento
- Proporciona tránsito confiable a través de un enlace físico
- Se ocupa del direccionamiento físico, la topología de red, el acceso a la red, la entrega ordenada de tramas y control de flujo
- Controla que no se pierdan datos innecesariamente
- Reparte la utilización del medio compartido entre las estaciones

- Trama o marco: unidad mínima de datos transferida entre entidades pares.

Red:

- Determina la mejor ruta para enviar la información (camino más corto, el más rápido o de menor tráfico)
- Controla la congestión de la red repartiendo la carga de manera equitativa entre las distintas rutas
- Convierte y adapta los mensajes entre redes heterogéneas
- Paquete: unidad mínima de información que se transfiere

Transporte:

- Tiene independencia total del tipo de red que se utilice
- Toma los datos procedentes del nivel de sesión y los pasa a la capa de red, asegurando que llegan correctamente al nivel de sesión del otro extremo
- Segmenta los datos originados en el host emisor y los re-ensambla en una corriente de datos dentro del sistema del host receptor
- Suministra servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte
- Proporciona confiabilidad del transporte entre dos hosts por lo que utiliza dispositivos de detección y recuperación de errores de transporte
- Proporciona servicio de comunicaciones por lo que establece, mantiene y termina adecuadamente los circuitos virtuales.
- Segmento: unidad mínima de información que se transfiere.

Sesión:

- Se establecen, administran y finalizan las conexiones de comunicación entre los dos extremos para el transporte ordinario de datos
- Proporciona servicio de reanudación de la conversación después de un fallo en la red o una interrupción
- Proporciona servicios a la capa de presentación
- Sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos

- Regula la sesión con disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Presentación:

- Controla el significado de la información que se transmite y permite la traducción de los datos entre las estaciones, es decir, convierte los datos entre emisor y receptor cuando estos utilizan códigos distintos
- Codifica y encripta datos en conversaciones confidenciales

Aplicación:

- Está en contacto directo con los programas o aplicaciones informáticas de las estaciones
- Es la capa más cercana al usuario
- Contiene los servicios de comunicación más utilizados en las redes
- No proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI.
- Establece la disponibilidad de los potenciales socios de comunicación
- Sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos
- Ejemplos: transferencia de archivos, correo electrónico, programas de hojas de cálculo, procesadores de texto, programas de terminales bancarias.

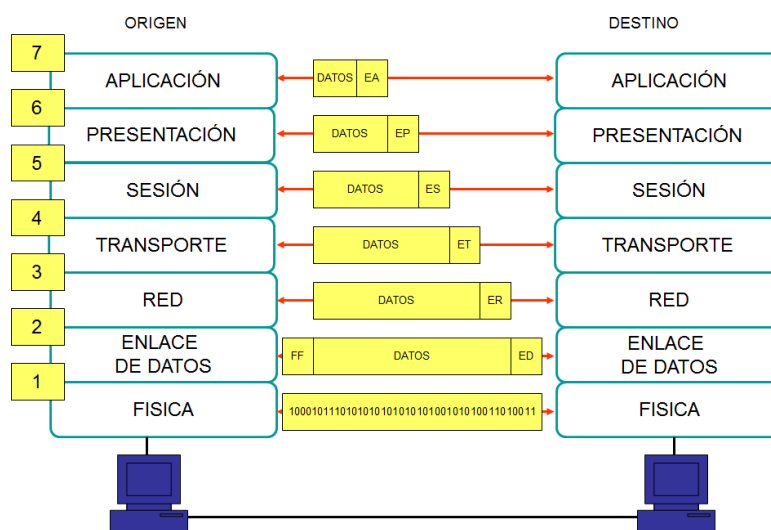


Figura 3. Encapsulamiento de la trama

4.4 Arquitectura TCP/IP

(TCP/IP) Protocolo de control de transmisión/Protocolo Internet, está construida de varios protocolos apilados por capas. Es la más utilizada del mundo y la base de comunicación de Internet. Tiene una topología irregular, la información se fragmenta para seguir rutas diferentes.

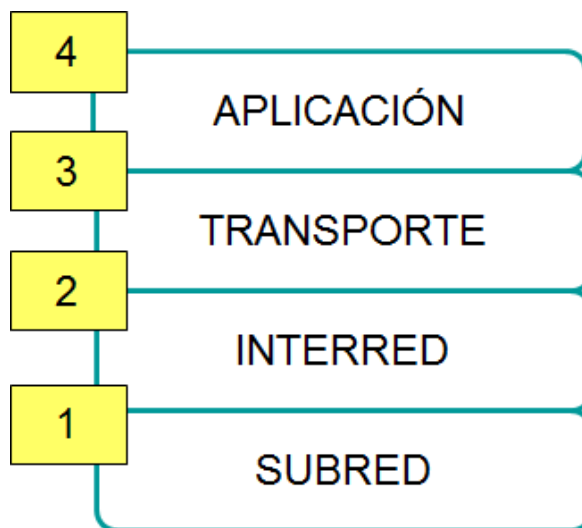


Figura 4. Modelo TCP/IP

4.4.1 Características

En 1973 el Departamento de Defensa de EE.UU. (DoD) creó el modelo TCP/IP con las siguientes características:

- Permitir interconectar redes diferentes.
- Ser tolerante a fallos: necesitaba una red que pudiera sobrevivir ante cualquier circunstancia.
- Permitir el uso de aplicaciones diferentes: transferencia de archivos, comunicación en tiempo real...
- Es independiente de los fabricantes y las marcas comerciales.
- Soporta múltiples tecnologías diferentes.
- Puede funcionar en máquinas de cualquier tamaño.
- Se ha convertido en estándar de comunicaciones desde 1983.

Redes:

- ARPANET: dedicada a la investigación. Se unieron universidades e instalaciones del gobierno.
- MILNET: de uso militar.

4.4.2 Funciones de los niveles TCP/IP

Subred:

- También denominada “Acceso a Red” o de “Host a Red”.
- Protocolo que conecta la estación de la red.
- Depende de la tecnología utilizada y no se especifica de antemano.
- Se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico.
- Incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.
- Facilita la técnica modular.

Interred:

- También conocida como capa de Internet.
- Permite que las estaciones envíen información (paquetes) a la red y los hagan viajar de forma independiente hacia su destino.
- Los paquetes pueden atravesar redes diferentes y llegar desordenados.
- No es responsable de ordenar los paquetes en el destino.
- Protocolo más importante el IP.
- Se produce la determinación de la mejor ruta y la conmutación de paquetes.

Transporte:

- Establece conversación entre origen y destino.
- Se encarga del control de errores y de la reordenación de los mensajes.
- Se define el protocolo TCP orientado a la conexión y fiable.
- Se define el protocolo UDP (Protocolo de Datagrama de Usuario) no orientado a la conexión y no fiable.

- Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos.

Aplicación:

- Contiene todos los protocolos de alto nivel que utilizan los programas para comunicarse:
 - TELNET: protocolo de terminal virtual.
 - FTP: protocolo de transferencia de archivos.
 - HTTP: protocolo usado en los navegadores para recuperar páginas Web.
- Maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo.

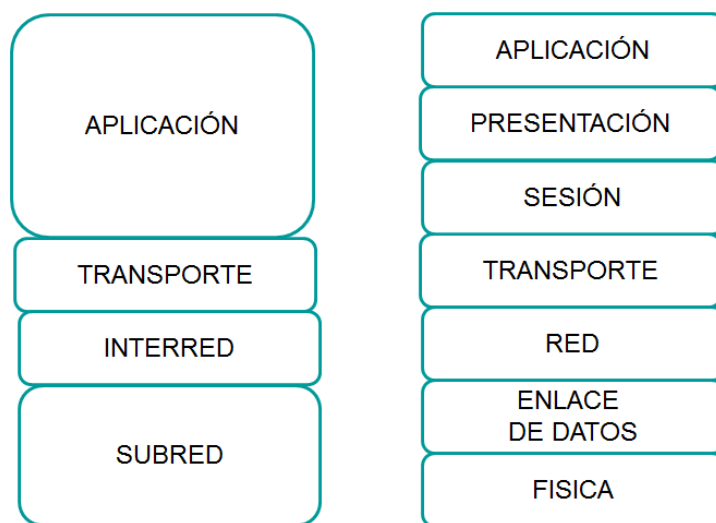


Figura 5. Comparación OSI Vs. TCP/IP

4.5 Hardware

4.5.1 Cables

El cableado es quien transporta físicamente las señales entre los PCs que integran la red. Su importancia radica tanto en su composición y en que se utilice.

Se han de tener en cuenta ciertos factores para elegir bien el cable para la red, algunos de estos factores son:

- La arquitectura de red (Ethernet, Token Ring, Arcnet, etc.) que se utilice, distancias que pueden unir el cable sin necesidad de usar repetidores.
- Las interferencias que puedan afectar al cable.
- El peso, tamaño, flexibilidad, facilidad y tiempo de instalación del cable y de los conectores hembra / macho disponibles para éste.
- La resistencia con el paso del tiempo, a los agentes externos que deterioran sus materiales
- La velocidad de transmisión de las señales, que puede soportar el cable en la red.

1000 BPS = 1 KBPS (Kilobits Por Segundo)

1000 KBPS = 1 MBPS (Megabits Por Segundo).

1000 MBPS = 1 GBPS (Giga Bits Por Segundo).

A menudo, se hace referencia al término “ancho de banda”, como sinónimo de velocidad de transmisión. En redes de área local “LAN” es común que las velocidades sean de 10 MBPS o 100 MBPS.

En redes con grandes distancias a cubrir, la variable que quizás más pesa en la elección del cableado es el costo económico.

4.5.1.1 Tipos de cables

4.5.1.1.1 Coaxial

Un cable coaxial consta de un núcleo de hilo de cobre rodeado por un aislante, un apantallamiento de metal trenzado y una cubierta externa. El termino apantallamiento hace referencia al trenzado o malla de metal que rodea algunos tipos de cable. El apantallamiento protege los datos transmitidos absorbiendo el ruido, de forma que no pasan por el cable y no distorsionan los datos. Al cable que contiene una lamina aislante y una capa de apantallamiento de metal trenzado se le denomina cable apantallado doble. Para entornos que están sometidos a grandes interferencias, se encuentra disponible un

apantallamiento cuádruple. Este apantallamiento consta de dos láminas aislantes y 2 capas de apantallamiento de metal trenzado.



Figura 6. Cable Coaxial

Hay dos tipos de cable coaxial:

- Fino (10Base2): es un cable coaxial flexible de unos 0,64 cm de grueso. Se puede utilizar para la mayoría de los tipos de redes, es un cable flexible y fácil de manejar. Puede soportar una señal de una distancia aproximada de 185 m, antes que la señal comience a sufrir atenuación. Está incluido en un grupo que se denomina la familia rg-58 y tiene una impedancia de 50 ohm.
- Grueso (10Base5): es un coaxial rígido de 1,27 cm a veces se le denomina ETHERNET estándar debido que fue el primer tipo de cable con la red Ethernet. Cuando mayor sea el grosor del núcleo de cobre, más lejos puede transportar las señales. Puede llevar una señal de 500 metros. Se utiliza como enlace central o backbone para conectar redes pequeñas basadas en thinnet.

Un TRANSCEIVER diseñado para Ethernet, thicknet incluye un conector conocido como VAMPIRO o FORADOR para establecer la conexión con el núcleo thicknet.

4.5.1.1.2 Par trenzado

Es el tipo de cable más común y se originó como solución para conectar teléfonos, terminales y ordenadores sobre el mismo cableado. Cada cable de este tipo está compuesto por una serie de pares de cables trenzados. Los pares se trenzan para reducir la interferencia entre pares adyacentes. Normalmente una serie de pares se agrupan en una única funda de color codificado para reducir el número de cables físicos que se introducen en un conducto. El número de pares por cable son 4, 25, 50, 100, 200 y 300. Cuando el número de pares es superior a 4 se habla de cables multipar.

Tipos:

- No apantallado (**UTP**): Es el cable de par trenzado normal y se le referencia por sus siglas en inglés UTP (Unshield Twisted Pair / Par Trenzado no Apantallado). Las mayores ventajas de este tipo de cable son su bajo costo y su facilidad de manejo. Sus mayores desventajas son su mayor tasa de error respecto a otros tipos de cable, así como sus limitaciones para trabajar a distancias elevadas sin regeneración. Para las distintas tecnologías de red local, el cable de pares de cobre no apantallado se ha convertido en el sistema de cableado más ampliamente utilizado. El segmento máximo de longitud de cable es de 100 metros.

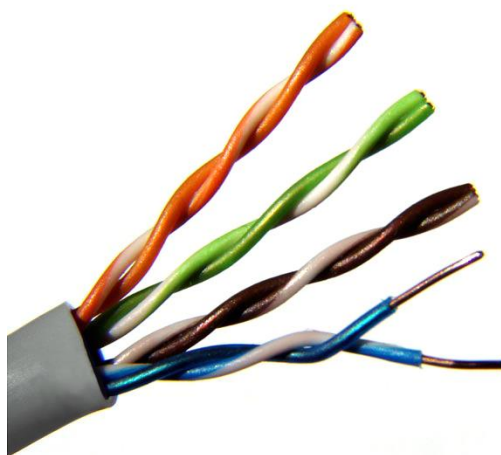


Figura 7. Cable de par trenzado UTP

Categoría	Impedancia	Frecuencia	Distancia	Uso
Cat 3	100 ohm	16 MHz	100 m.	10 Mbps
Cat 4	100 ohm	20 MHz	100 m.	10/100 Mbps
Cat 5	100 ohm	100 MHz	100 m.	10/100 Mbps
Cat 5e	100 ohm	100 MHz	350 m.	100/1000 Mbps
Cat 6	100 ohm	250 MHz	100 m.	1000 Mbps

Tabla 1. Comparativa categorías cable par trenzado

- Apantallado (**STP**): Cada par se cubre con una malla metálica, de la misma forma que los cables coaxiales, y el conjunto de pares se recubre con una lámina apantallante. Se referencia frecuentemente con sus siglas en inglés STP (Shield Twisted Pair / Par Trenzado Apantallado). El empleo de una malla apantallante reduce la tasa de error, pero incrementa el coste al requerirse un proceso de fabricación más costoso.

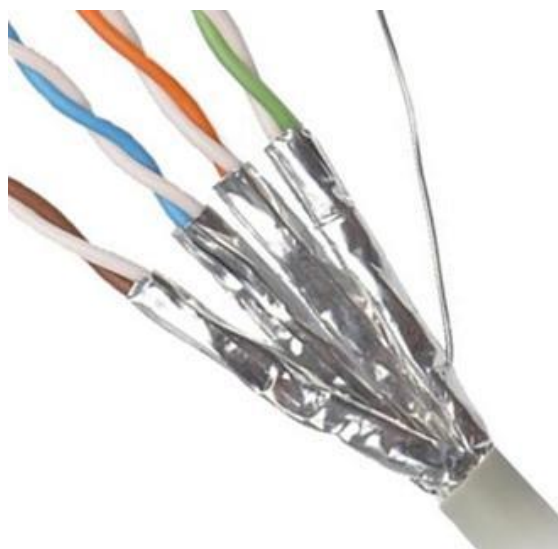


Figura 8. Cable de par trenzado STP

- Uniforme (**FTP**): Cada uno de los pares es trenzado uniformemente durante su creación. Se realiza un apantallamiento global de todos los pares mediante una lámina externa apantallante. Esta técnica permite

tener características similares al cable apantallado. Este es usado dentro de la categoría 5 y 5e (Hasta 100 MHz).

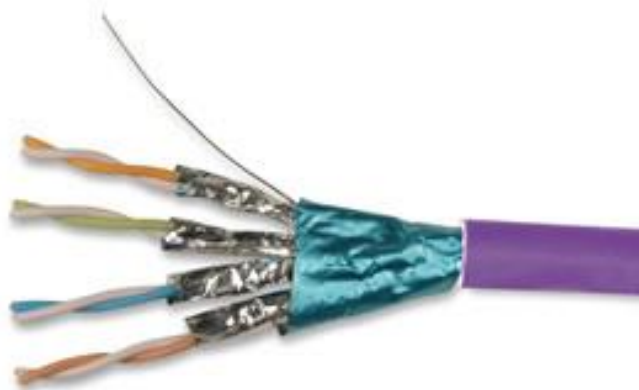


Figura 9. Cable de par trenzado FTP

4.5.1.1.3 Fibra óptica

Este cable está constituido por uno o más hilos de fibra de vidrio. La luz producida por diodos o por láser, viaja a través del núcleo debido a la reflexión que se produce en la cubierta, y es convertida en señal eléctrica en el extremo receptor. La fibra óptica es un medio excelente para la transmisión de información debido a sus excelentes características. Su mayor desventaja es su coste de producción superior al resto de los tipos de cable, debido a necesitarse el empleo de vidrio de alta calidad y la fragilidad de su manejo en producción. La terminación de los cables de fibra óptica requiere un tratamiento especial que ocasiona un aumento de los costes de instalación.

1. Fibra óptica
2. Protección secundaria (holgada o densa)
3. Elemento de tracción (aramida o fibra de vidrio)
4. Cubierta interna (PVC, polietileno...)
5. Coraza
6. Cubierta exterior (PVC, polietileno...)

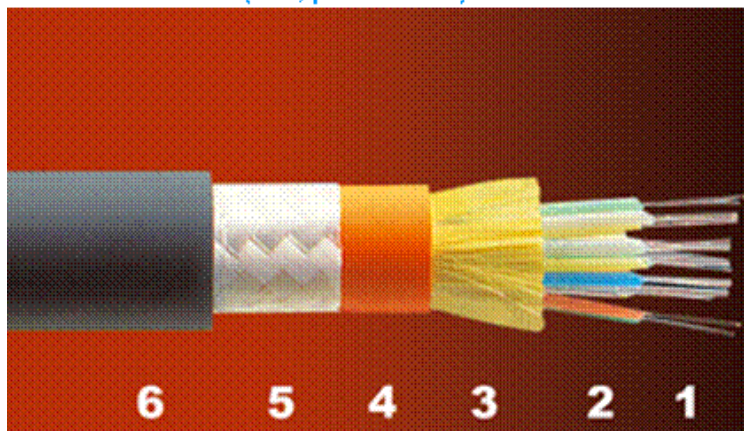


Figura 10. Cable de Fibra Óptica

4.5.1.1.3.1 Características

- Ancho de banda: La fibra óptica proporciona un ancho de banda significativamente mayor que los cables de pares (UTP /STP) y el Coaxial.
- Integridad de datos: En condiciones normales, una transmisión de datos por fibra óptica tiene una frecuencia de errores o BER (Bit Error Rate) menor de $10 \text{ E-}11$.
- Duración: La fibra óptica es resistente a la corrosión y a las altas temperaturas.
- Seguridad: Debido a que la fibra óptica no produce radiación electromagnética, es resistente a las acciones intrusivas de escucha.

4.5.1.1.3.2 Tipos

- Monomodo: Son aquellas que por su especial diseño pueden guiar y transmitir un solo rayo de luz (un modo de propagación) y tiene la particularidad de poseer un ancho de banda elevadísimo.
- Multimodo: Son aquellas que pueden guiar y transmitir varios rayos de luz por sucesivas reflexiones, (modos de propagación). La palabra modo significa trayectoria.



Figura 11. Tipos de cable de Fibra Óptica

4.5.2 Dispositivos de red

Son todos aquellos que se conectan de forma directa a un segmento de red. Estos dispositivos están clasificados en dos grandes grupos el primero son los dispositivos de usuario final entre los cuales destacan las computadoras, escáneres, impresoras etc. Por otro lado tenemos los dispositivos de red estos dispositivos son los que conectan los dispositivos de usuario final posibilitando la comunicación entre ellos.

4.5.2.1 Hubs (concentrador)

El hub es el dispositivo de conexión más básico. Es utilizado en redes locales con un número muy limitado de máquinas. No es más que una toma múltiple RJ45 que amplifica la señal de la red (base 10/100). Es el dispositivo que permite centralizar el cableado de una red de computadoras, para luego poder ampliarla. Trabaja en la capa física (capa 1) del modelo OSI o la capa de acceso al medio en el modelo TCP/IP. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos (repetidor).

Los concentradores no logran dirigir el tráfico que llega a través de ellos, y cualquier paquete de entrada es transmitido a otro puerto (que no sea el puerto de entrada), y por eso aparecen las colisiones de paquetes como resultado, que impiden en gran medida la fluidez del tráfico. Cuando dos dispositivos intentan comunicar simultáneamente, ocurrirá una colisión entre los paquetes transmitidos, que los dispositivos transmisores detectan. Al detectar esta colisión, los dispositivos dejan de transmitir y hacen una pausa antes de volver a enviar los paquetes.

En la actualidad, la tarea de los concentradores la realizan, con frecuencia, los conmutadores (Switches).



Figura 12. Hubs

4.5.2.2 Switches (conmutador)

También llamados Conmutadores es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta. Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo

retransmiten la información hacia los tramos en los que están los destinatarios de la trama, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

Básicamente constan de N bocas donde se conectan entre 1 y N dispositivos. Cuenta con una memoria interna para almacenar la relación entre la boca y las direcciones MAC de los dispositivos asociados a ella y otra memoria que almacena las tramas recibidas antes de ser enviadas al destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por lo tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

Uno de los puntos críticos de estos equipos son los bucles, que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.



Figura 13. Switch

4.5.2.3 Routers (enrutador)

Es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de

datos entre ellas o determinar la mejor ruta que deben tomar. Opera en la capa tres del modelo OSI.

Los primeros modelos en los años 80 permitían multiprotocolo, pero actualmente, se usa masivamente IP en la capa de red y los dispositivos multiprotocolo se han quedado obsoletos.

El funcionamiento básico de un router, como se deduce de su nombre, consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. Con arreglo a esta información reenvía los paquetes a otro router o bien al destino, en una actividad que se denomina '**encaminamiento**'. Cada router se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto, como protocolos basado en el algoritmo de Dijkstra.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- **Reenvío de paquetes:** cuando un paquete llega al enlace de entrada de un router, éste tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los routers es que no difunden tráfico en broadcast.
- **Encaminamiento de paquetes:** mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.

Por tanto, debemos distinguir entre reenvío y encaminamiento. Reenvío consiste en coger un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla.

Tanto los routers como los anfitriones guardan una tabla de enrutamiento. El proceso de enrutamiento de cada sistema actualiza la tabla con todas las rutas conocidas. El sistema lee la tabla de enrutamiento antes de reenviar paquetes a la red local. La tabla de enrutamiento enumera las direcciones IP de las redes que conoce el sistema, incluida la red local predeterminada del sistema.



Figura 14. Routers

4.5.2.3.1 Tipos de enrutamiento

4.5.2.3.1.1 Enrutamiento estático

Hosts y redes de tamaño reducido que obtienen las rutas de un router predeterminado, y routers predeterminados que sólo necesitan conocer uno o dos routers.

Determinación del enrutamiento: La información de enrutamiento que el router aprende desde sus fuentes se coloca en su propia tabla de enrutamiento. El router se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino. La tabla de enrutamiento es la fuente principal de información del enrutador acerca de las diferentes redes. Si la red de destino está conectada directamente, el router ya sabrá el puerto que debe usar para reenviar los paquetes. Si las redes de destino no están conectadas directamente, el router debe aprender y calcular la ruta más óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se constituye mediante uno de estos dos métodos o ambos:

- Manualmente, por el administrador de la red.
- A través de procesos dinámicos que se ejecutan en la red.

Rutas estáticas: Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso de enrutamiento según los parámetros del administrador.

Las rutas estáticas por defecto especifican una puerta de enlace de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir, se desconoce.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento. La ruta estática se configura para conseguir conectividad con un enlace de datos que no esté directamente conectado al router. Para conectividad de extremo a extremo, es necesario configurar la ruta en ambas direcciones. Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento.

4.5.2.3.1.2 Enrutamiento dinámico

El enrutamiento dinámico le permite a los routers ajustar, en tiempo real, los caminos utilizados para transmitir paquetes IP. Cada protocolo posee sus propios métodos para definir rutas (camino más corto, utilizar rutas publicadas por pares, etc.).

4.5.2.4 Puntos de acceso (Wireless Access Point)

Un punto de acceso inalámbrico (conocido por las siglas WAP o AP), en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación alámbrica para formar una red inalámbrica que interconecta dispositivos móviles o con tarjetas de red inalámbricas.

Los WAP son dispositivos que permiten la conexión inalámbrica de un dispositivo móvil (PC, Smartphone, tablet) con una red. Normalmente, un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red tanto cableada como inalámbrica.

Los WAP tienen asignadas direcciones IP, para poder ser configurados.

Muchos WAP pueden conectarse entre sí para formar una red aún mayor.

Generalmente, los AP tienen como **función principal** permitir la conectividad con la red, delegando la tarea de ruteo y direccionamiento a servidores, routers y switches. La mayoría de los AP siguen el estándar de comunicación, 802.11 de la IEEE, lo que permite una compatibilidad con una

gran variedad de equipos inalámbricos. Al fortalecer la interoperabilidad entre los servidores y los AP, se pueden lograr mejoras en el servicio que ofrecen, por ejemplo, la respuesta dinámica ante cambios en la red y ajustes de la configuración de los dispositivos.

Los AP son el enlace entre las redes cableadas y las inalámbricas. El surgimiento de estos dispositivos ha permitido el ahorro de nuevos cableados de red. Un AP con el estándar IEEE 802.11b tiene aproximadamente un radio de 100 m.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la red de área local inalámbrica (WLAN) y la red de área local (LAN) cableada.

Un único AP puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros. Este o su antena normalmente se colocan en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores situados en sus equipos (PC, smart TV, tablet, smartphone, radio por Internet, etc...). Estos proporcionan una interfaz entre el SO de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica.



Figura 15. Punto de Acceso

4.6 LAN WIFI

Una red de área local inalámbrica, también conocida como WLAN (wireless local area network), es un sistema de comunicaciones inalámbricas flexibles, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

Estas redes tienen ciertas **ventajas** con respecto a las cableadas:

- Permiten movilidad.
- Son flexibles, ideales para instalaciones temporales.
- Son fáciles de instalar.
- Permiten su integración con sistemas cableados.

Al igual que tienen ciertas **desventajas**:

- Velocidad: Otro de los problemas que presenta este tipo de redes es que actualmente alcanzan la velocidad que obtienen las redes de datos cableadas.

Además, en relación con el apartado de seguridad, el tener que cifrar toda la información supone que gran parte de la información que se transmite sea de control y no información útil para los usuarios, por lo que incluso se reduce la velocidad de transmisión de datos útiles y no se llega a tener un buen acceso.

- Seguridad: Se han de tomar medidas de seguridad para que no todo el mundo pueda conectarse a un PA con un terminal inalámbrico, dichas medidas van encaminadas en dos sentidos: por una parte está el cifrado de los datos que se transmiten y en otro plano, pero igualmente importante, se considera la autenticación entre los diversos usuarios de la red.

4.6.1 Estándares WIFI

4.6.1.1 IEEE 802.11

El estándar IEEE 802.11 es una frecuencia de radio desarrollado por el IEEE (Institute of Electrical and Electronics Engineers), y la mayoría de los sistemas operativos lo soportan, así como muchos de los portátiles, móviles de última generación, consolas, impresoras y otros periféricos. Este protocolo fue creado en el año 1997 y existen varias clases de este estándar que se pueden ver a continuación

4.6.1.1.1 802.11a

Creado en 1997 el estándar 802.11 con velocidades de transmisión de 2Mb/seg, hasta que en 1999 desarrollaron el estándar 802.11a que era una revisión del estándar original y que utiliza el mismo juego de protocolos de base que este. También llamado WiFi 5, el estándar 802.11a opera en la banda de 5 GHz que está menos congestionada y utiliza la modulación OFDM (orthogonal frequency-division multiplexing) con 52 subportadoras, lo que le infiere dos notables ventajas respecto al 802.11b: incrementa la velocidad máxima de transferencia de datos por canal (de 11 Mbps a 54 Mbps) y aumenta el número de canales sin solapamiento.

Pero el uso de esta banda también tiene sus desventajas, puesto que restringe el uso de los equipos 802.11a sólo a puntos en línea de vista, siendo necesario la instalación de un mayor número de puntos de acceso 802.11a para cubrir la misma zona; debido a esto las ondas no pueden penetrar tan lejos como los del estándar 802.11b, ya que estas son más fácilmente absorbidas por las paredes y otros objetos sólidos en su camino pues su longitud de onda es menor.

Características principales:

- Emite a una velocidad de 54 Mb/seg (megabytes por segundo).
- Volumen de información (Throughput) de 27 Mb/seg.
- Banda de frecuencia de 5 GHz.

4.6.1.1.2 802.11b

Uno de los más usados, desarrollado en 1999, es una extensión directa de la técnica de modulación definida en el estándar original 802.11. Su

espectacular incremento en throughput (volumen de información que fluye a través de las redes de datos) comparado con el estándar original junto con sustanciales reducciones de precios ha llevado a la rápida aceptación de 802.11b como la tecnología inalámbrica LAN definitiva.

Como desventaja los dispositivos 802.11b sufren interferencias de otros productos operando en la banda 2.4 GHz, como pueden ser hornos microondas, dispositivos Bluetooth, monitores de bebés y teléfonos inalámbricos. Por otro lado, los productos de estándar 802.11b no son compatibles con los productos de estándar 802.11a por operar en bandas de frecuencia distintas.

Características principales:

- Emite a una velocidad de 11 Mb/seg.
- Volumen de información (Throughput) de 5 Mb/seg.
- Banda de frecuencia de 2,4 GHz.

4.6.1.1.3 802.11g

Desarrollado en 2003, el 802.11g es el tercer estándar de modulación y la evolución del 802.11b, es además el más usado en la actualidad. Los productos IEEE 802.11g poseen un alto grado de compatibilidad con versiones anteriores pues trabaja en la banda de 2.4 GHz como 802.11b, pero usa el mismo esquema de transmisión basado en OFDM como 802.11a, utilizando 48 subportadoras.

802.11g fue rápidamente adoptado por los consumidores en Enero de 2003, antes de su ratificación en Junio, debido al deseo de velocidades de transmisión superiores y reducciones en los costes de fabricación. Para el verano de 2003, la mayoría de los productos de doble banda 802.11a/b pasaron a ser dual-band/tri-mode (doble banda/tres modos), esto quiere decir que pueden funcionar en la banda de 2.4 GHz o de 5 GHz y en cualquiera de los tres modos aceptados por la IEEE: el a, b y g.

Como el estándar 802.11b, los dispositivos de estándar 802.11g les afectan las interferencias de otros productos operando en la banda de 2.4 GHz.

Características principales:

- Emite a una velocidad de 54 Mb/seg.
- Volumen de información (Throughput) de 22 Mb/seg.

- Banda de frecuencia de 2.4 GHz.

4.6.1.1.4 802.11n

El estándar 802.11n es una ratificación que mejora los previos estándares 802.11 añadiendo la tecnología MIMO que son antenas Multiple-Input Multiple-Output, unión de interfaces de red (Channel Bonding), además de agregación de marco a la capa MAC.

MIMO genera cuatro canales de tráfico simultáneos de 72.2 Mbps para enviar y recibir datos a través de la incorporación de varias antenas.

Channel Bonding, también conocido como canal 40 MHz, puede usar simultáneamente dos canales separados no superpuestos de 20 MHz, lo que permite incrementar enormemente la velocidad de datos transmitidos.

Uso simultáneo de las bandas de frecuencia de 2,4 GHz y de 5,4 GHz que hace que sea compatible con dispositivos basados en todas las ediciones anteriores de WiFi.

La velocidad real de transmisión a la que se podría llegar es 600 Mbps, que es 10 veces más rápida que bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que bajo el estándar 802.11b.

802.11n fue aprobada por la IEEE el 11 de Septiembre de 2009.

Características principales:

- Emite a una velocidad de 600 Mb/seg.
- Volumen de información (Throughput) de 144 Mb/seg.
- Bandas de frecuencia: 2,4 GHz y 5 GHz.

Normas (capa física y de acceso al medio)	Velocidad transmisión máxima (Mbps)	Throughput máximo típico (Mbps)	Numero máximo de redes colocalizadas	Banda de frecuencia	Radio de cobertura típico (interior)	Radio de cobertura típico (exterior)
IEEE 802.11a/h	54 Mbps	22 Mbps	14 (5.7 GHz)	5 GHz	85 m	185 m
IEEE 802.11b	11 Mbps	6 Mbps	3	2.4 GHz	50 m	140 m
IEEE 802.11g	54 Mbps	22 Mbps	3	2.4 GHz	65 m	150 m
IEEE 802.11n (40 MHz)*	>300 Mbps	>100 Mbps	1 (2.4 GHz) 7 (5.7 GHz)	5 GHz	120 m	300 m
IEEE 802.11n (20 MHz)*	144 Mbps	74 Mbps	3 (2.4 GHz) 14 (5.7 GHz)	2.4 GHz y 5 GHz	120 m	300 m

Tabla 2. Comparación estándares 802.11

4.7 Seguridad

En las redes wifi o inalámbricas, uno de los factores más delicados es el de la seguridad, normalmente los administradores con poca experiencia dejan los valores predeterminados de los PA o de los routers, esto hace que sus redes sean objetivo de ataques externos para poder controlarla. En este apartado vamos a ver las técnicas más comunes para hacer que tu red sea más segura y que la misma sea solo utilizada por los usuarios para los que ha sido diseñada.

Siguiendo unas pautas muy sencillas podemos hacer nuestra red más segura:

- Cambiar frecuentemente la contraseña de acceso y utilizar caracteres diversos como mayúsculas, minúsculas, signos de puntuación, números...
- Se debe modificar el SSID (Identificador de red que comparten todos los paquetes de datos de dicha red) que viene predeterminado.
- Desactivar el broadcasting SSID y DHCP.
- Configurar los dispositivos conectados con su IP (indicando específicamente qué dispositivos están autorizados para conectarse).
- Utilización de cifrado.
- Filtrar los dispositivos conectados mediante la MAC address.

La seguridad de una red wifi puede ser puesta a prueba mediante una auditoria de wifi. Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

4.7.1 Protocolos de cifrado

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares wifi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos.

4.7.1.1 WEP

WEP, acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite a cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

Comenzando en 2001, varias debilidades serias fueron identificadas. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. A pesar de sus debilidades, WEP sigue siendo utilizado, ya que es a menudo la primera opción de seguridad que se presenta a los usuarios por las herramientas de configuración de los routers aun cuando sólo proporciona un nivel de seguridad que puede disuadir del uso sin autorización de una red privada, pero sin proporcionar verdadera protección. Fue desaprobado como un mecanismo de privacidad inalámbrico en 2004, pero todavía está documentado en el estándar actual.

WEP es a veces interpretado erróneamente como Wireless Encryption Protocol.

4.7.1.2. WPA

WPA, Wi-Fi Protected Access (en español «Acceso Wi-Fi protegido»), es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, WEP. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por la Wi-Fi Alliance («Alianza Wi-Fi»).

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave precompartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

Presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.

Un inconveniente encontrado en la característica agregada al Wi-Fi llamada Wi-Fi Protected Setup (también bajo el nombre de QSS) permite eludir la seguridad e infiltrarse en las redes que usan los protocolos WPA y WPA2.

4.7.1.3. WPA2

WPA2 (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

El estándar 802.11i fue ratificado en junio de 2004.

La Wi-Fi Alliance llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos

certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.

4.7.1.4. IPsec

IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Esto sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. Una ventaja importante es que para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

IPsec consta de tres protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

- Authentication Header (AH) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.
- Encapsulating Security Payload (ESP) proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.
- Internet key exchange (IKE) emplea un intercambio secreto de claves de tipo Diffie-Hellman para establecer el secreto compartido de la sesión. Se suelen usar sistemas de Criptografía de clave pública o clave pre-compartida.

4.7.1.5. DES

Los algoritmos criptográficos definidos para usar con IPsec incluyen HMAC-SHA-1 para protección de integridad, y Triple DES-CBC y AES-

CBC para confidencialidad. DES (Data Encryption Standard, estándar de cifrado de datos) es un algoritmo desarrollado originalmente por IBM a requerimiento del NBS (National Bureau of Standards, Oficina Nacional de Estandarización, en la actualidad denominado NIST, National Institute of Standards and Technology, Instituto Nacional de Estandarización y Tecnología) de EE.UU. y posteriormente modificado y adoptado por el gobierno de EE.UU. en 1977 como estándar de cifrado de todas las informaciones sensibles no clasificadas. Posteriormente, en 1980, el NIST estandarizó los diferentes modos de operación del algoritmo. Es el más estudiado y utilizado de los algoritmos de clave simétrica.

El nombre original del algoritmo, tal como lo denominó IBM, era Lucifer. Trabajaba sobre bloques de 128 bits, teniendo la clave igual longitud. Se basaba en operaciones lógicas booleanas y podía ser implementado fácilmente, tanto en software como en hardware. Tras las modificaciones introducidas por el NBS, consistentes básicamente en la reducción de la longitud de clave y de los bloques, DES cifra bloques de 64 bits, mediante permutación y sustitución y usando una clave de 64 bits, de los que 8 son de paridad (esto es, en realidad usa 56 bits), produciendo así 64 bits cifrados.

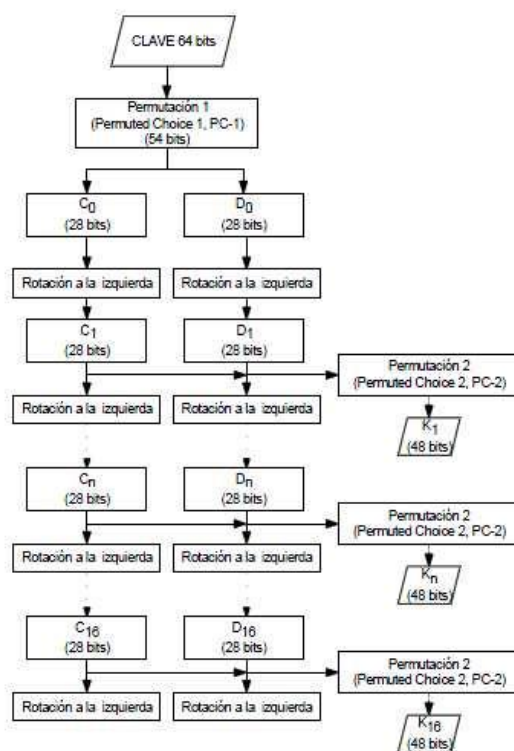


Figura 16. Cálculo de subclaves, Ki

Como se acaba de ver en la figura, DES tiene 19 etapas diferentes. La primera etapa es una transposición, una permutación inicial (IP) del texto plano de 64 bits, independientemente de la clave. La última etapa es otra transposición (IP-1), exactamente la inversa de la primera. La penúltima etapa intercambia los 32 bits de la izquierda y los 32 de la derecha. Las 16 etapas restantes son una Red de Feistel de 16 rondas. En cada una de las 16 iteraciones se emplea un valor, K_i , obtenido a partir de la clave de 56 bits y distinto en cada iteración.

Se realiza una permutación inicial (PC-1) sobre la clave, y luego la clave obtenida se divide en dos mitades de 28 bits, cada una de las cuales se rota a izquierda un número de bits determinado que no siempre es el mismo. K_i se deriva de la elección permutada (PC-2) de 48 de los 56 bits de estas dos mitades rotadas.

Por otro lado, la función f de la red de Feistel se compone de una permutación de expansión (E), que convierte el bloque correspondiente de 32 bits en uno de 48. Después realiza una or-exclusiva con el valor K_i , también de 48 bits, aplica ocho SCajas de 6×4 bits, y efectúa una nueva permutación (P).

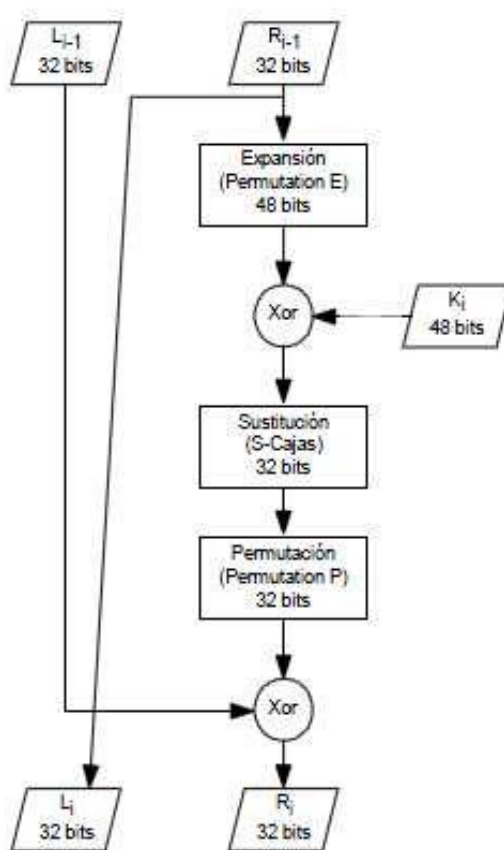


Figura 17. Ronda del algoritmo DES

Para descifrar basta con usar el mismo algoritmo empleando las Ki en orden inverso.

4.7.1.6. AES

AES conocida como Estándar de Encriptación Avanzada (Advanced Encryption Standard). AES es una técnica de cifrado de clave simétrica que remplazará el Estándar de Encriptación de Datos (DES) utilizado habitualmente.

Es el resultado de un llamamiento a nivel mundial por la presentación de solicitudes de los algoritmos de cifrado emitido por el Instituto Nacional de Estándares y Tecnología (NIST) del Gobierno de EEUU en el año 1997 y completado en el año 2000.

El algoritmo ganador, Rijndael, fué desarrollado por dos criptólogos Belgas, Vincent Rijmen y Joan Daemen.

AES proporciona una encriptación segura y ha sido elegida por NIST como un Estándar de Proceso de Información Federal en Noviembre del 2001 (FIPS-197), y en Junio del 2003 el Gobierno de EEUU (NSA) anunció que AES es lo suficientemente seguro para proteger la información clasificada hasta el nivel ALTO SECRETO, que es el nivel más alto de seguridad y que se definen como información que pudiera causar "daños excepcionalmente graves" a la seguridad nacional en caso de ser divulgada al público.

El algoritmo AES utiliza una de las tres fortalezas de clave de cifrado: una clave de encriptación (contraseña) de 128, 192, o 256 bits. Cada tamaño de la clave de cifrado hace que el algoritmo se comporte ligeramente diferente, por lo que el aumento de tamaño de clave no sólo ofrece un mayor número de bits con el que se pueden cifrar los datos, sino también aumentar la complejidad del algoritmo de cifrado.

BitZipper soporta claves de cifrado de 128 y 256 bits, las cuales son soportadas por WinZip 9. Ambas claves proporcionan una seguridad mayor respecto a la encriptación estándar ZIP 2.0. Es ligeramente más rápido de encriptar y desencriptar datos protegidos con AES 128-bit, pero con los PCs rápidos de hoy en día la diferencia de tiempo apenas se percibe.

AES opera en una matriz de 4x4 bytes, llamada state y que pasamos a ver:

SubBytes: en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda.

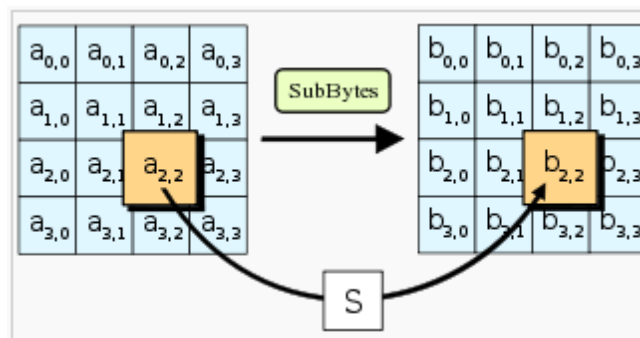


Figura 18. Etapa SubBytes

ShiftRows: en este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.

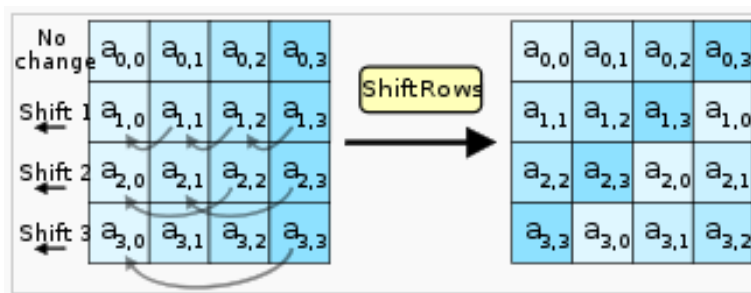


Figura 19. Etapa ShiftRows

MixColumns: operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.

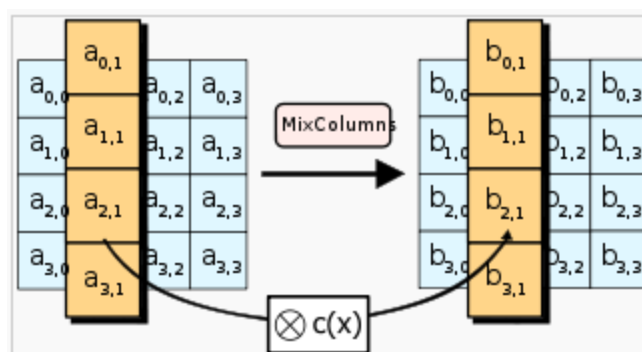


Figura 20. Etapa MixColumns

AddRoundKey: cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.

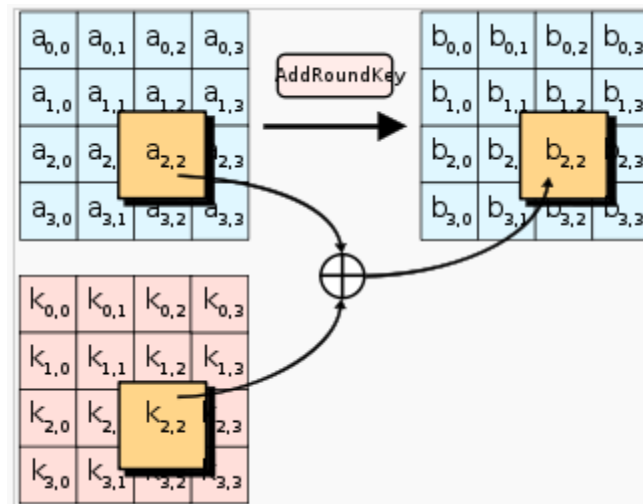


Figura 21. Etapa AddRoundKey

5. Diseño de la Red

En este capítulo se pasa a detallar los equipos elegidos para la red, así como su ubicación.

5.1 Descripción del entorno

El centro de enseñanza ficticio objeto de este PFC está formado por un edificio de 3 plantas además de una Planta -1, en el cual no habrá señal WIFI. Tanto la red cableada como el enlace wifi formaran una sola red Ethernet con el mismo direccionamiento IP.

En las aulas se colocarán 2 puntos de red uno para el equipo del profesor y otro punto para futuras necesidades. El equipo del profesor dispondrá además de una PDI (pizarra digital interactiva) y podrá ser usada como pizarra convencional con rotuladores específicos y para proyectar presentaciones, mostrar a los alumnos páginas web o aplicaciones, etc...

Por otro lado habrá varios puntos de red concentrados en las aulas de informática y otros más repartidos por despachos, aulas de docencia especial...

En el área ocupada por la sala de profesores y secretaria hay más puntos de red que equipos previstos a instalar inicialmente porque las impresoras que usaran los profesores y la dirección del centro se colocarán en esos puntos físicos. Por otro lado se colocaran puntos de red adicionales en los lugares donde se van a ubicar los AP para el enlace wifi.

La distribución de los puntos de red en el edificio se realizará de acuerdo a las tablas 5.1. En ella se indica los puntos de red conmutados, es decir, los que están conectados a un switch. En las diferentes figuras del anexo A se puede apreciar donde está concretamente cada estancia dentro de cada edificio y situarla mejor.

EDIFICIO PRINCIPAL	
ESTANCIA	PUNTOS DE RED
PLANTA BAJA(68)	
Aulas de Infantil (1-10)	20
Aula Polivalente ESO Aula Informática	28
Relaciones Externas	2
Secretaría	2
Administración	2
Dirección	2
Coordinación infantil	2
Tutoría	2
Sala de profesores	8
PLANTA PRIMERA (74)	
Aulas de Primaria (1-12)	24
Despacho Coordinación Primaria	2
Sala de profesores	8
Despacho Coordinador	2
Tutoría	2
Laboratorio ESO	2
Aula Polivalente ESO Aula Informática	28
Biblioteca Primaria y ESO	6
PLANTA SEGUNDA (70)	
Aulas Primaria (13-18)	12
Aulas Polivalentes ESO (1-3)	6
Aula Polivalente ESO (12) Aula Informática	28
Taller Tecnología Bachillerato	2
Sala Profesores	8
Aula Pequeño Grupo EPO(1-6)	12
Taller Polivalente ESO y Primaria	2

Tabla 3. Desglose de puntos de red

5.2 Distribución de los elementos de la red

En el edificio se montará una troncal o backbone que unirá todos los switches de todas las plantas. El cable de red que una los switches será de un color claramente diferente al que llegue desde los puntos de red a cada armario, así será muy sencillo distinguir el cableado de la troncal que une los switches del cableado que forma la red de los puestos de trabajo. Por otro lado, todos los puntos de red de cada planta se unirán a su switch correspondiente en esa misma planta en una topología de estrella.

En principio, la troncal estará formada por un sólo cable UTP que una todos los switches, pero los switches elegidos disponen de la posibilidad de hacer trunk con sus puertos, por lo que podrían ponerse enlaces de 2 ó 4 Gbps por ejemplo en la troncal frente a 1 Gbps en los puntos de red. Esto requerirá el uso de tantas bocas en el switch como velocidad queramos en el enlace trunk. Si queremos 2 Gbps necesitaremos usar 2 bocas, si queremos 4 Gbps, 4 bocas y así sucesivamente. Al final el enlace trunk creado se comportará como una sola boca a la velocidad definida.

El principio, con un sólo enlace de 1 Gbps en la troncal será más que suficiente para soportar el tráfico previsto en la red, a pesar de que la velocidad entre switches sea igual a la de los puntos de red. En cualquier caso, ampliar este factor en el futuro no es complicado y resulta económico. Se plantea esa posibilidad más adelante, en el apartado correspondiente.

La troncal atravesará el forjado del edificio longitudinalmente desde la planta baja hacia arriba, hacia la planta sótano no hay ningún tipo de red ni cableada ni inalámbrica. Este despliegue será sencillo ya que los armarios que formarán los nodos de la troncal se colocarán estratégicamente para que queden unos encima de otros entre plantas. El cable que suba de un armario a otro se protegerá con una canaleta vertical, de este modo quedará disimulada estéticamente y se conseguirán minimizar además golpes y manipulaciones. Hay que evitar que la canaleta quede en mitad de una pared, ya que estaría más desprotegida y sería más vulnerable frente a impactos incontrolados por parte de los alumnos, etc.

El cableado desde cada uno de los puntos de red hacia el nodo de la troncal situada en cada planta se realizará, en la medida de lo posible, a través de dos canaletas paralelas al pasillo en sus extremos y sujetas al techo, de modo que de cada aula salgan los cables UTP correspondientes a los puntos de red hacia esa canaleta y desde allí hacia el armario correspondiente a esa planta.

Los rack se colocaran en la parte de atrás de las salas de informática, como se puede ver en el anexo A, todos los equipos de la planta estarán unidos al switch dentro de ese armario y en topología de estrella. Para la unión entre switches, se usarán los últimos puertos de cada conmutador, en este caso la boca número 48, mientras que para los puntos de red, se usarán las bocas 1 y siguientes. De este modo, si se amplía el ancho de banda de la troncal mediante trunking en el futuro se podrán usar las bocas 47, 46, etc respetando los colores asignados a dicha troncal, dando lugar a una instalación mucho más limpia, clara y organizada.

Cada nodo constará de un armario tipo rack mural de 19" y 15 unidades. Los armarios serán de dos cuerpos, puerta de cristal y cerraduras en puerta y en lateral para mayor seguridad. El sistema de doble cuerpo, que mejora notablemente la accesibilidad a los elementos internos puede ser apreciado en la figura 5.2.



Figura 22. Armario mural de 19" con doble cuerpo y llave

Dentro del armario y con carácter general se dispondrá de 3 patch-panel, 2 pasa hilos, 1 switch de 48 bocas (6 Unidades en total) y una regleta de 6 tomas con interruptor con soporte hasta 16A (1 Unidad), dejando las unidades restantes para adaptaciones especiales como se verá más adelante o para posibles futuras ampliaciones. El armario tendrá ventilación artificial superior (integrada sin ocupación de unidades) y estará colocado en la pared, lo más pegado al techo posible para evitar el fácil acceso de las personas que transitan por allí, dejando unos 20 ó 25 cm entre el techo y la parte superior del armario para no dificultar la respiración del mismo. Es importante resaltar el tema de la ventilación, ya que al no encontrarse los equipos en un CPD apropiadamente climatizado, hay que procurar que la electrónica no sufra en exceso. Dentro de los márgenes posibles, se procura colocar lejos de fuentes de calor como tuberías de calefacción, ventanas por las que entre el sol directamente, etc....

El armario de la planta baja dispondrá además de una bandeja para colocar apropiadamente el modem-router de salida a Internet, ya que el PTR (Punto de Terminación de Red) que da acceso a Internet a través de Fibra Óptica se encuentra justo al lado del lugar elegido para la colocación del armario. El armario dispondrá de llave para cada uno de los cuerpos, así se garantizará la imposibilidad de manipulación por parte de alumnos o profesores.

La electrónica de red se repartirá en los armarios por todo el centro según la distribución de la tabla 5.2.

Edificio principal	
Ubicación	Electrónica
Planta Baja	2 X Switches de 48 bocas 1 X Router
Planta primera	2 X Switches de 48 bocas
Planta segunda	2 X Switches de 48 bocas

Tabla 4. Desglose del reparto de electrónica de red en los armarios

Desde el punto de vista técnico y de contenido, los armarios serán del mismo modelo y con elementos iguales (a excepción del router en la planta baja) de esta manera cualquier modificación o ampliación será más sencilla de realizar según las necesidades del centro educativo.

En todos los casos los armarios tendrán refrigeración superior sin ocupación de unidad a través de un ventilador sencillo. Por otro lado, la primera unidad de todos los armarios se dejará vacía para mejorar el flujo de aire interno y conseguir una mejor refrigeración, permitiendo la posibilidad futura de instalar un kit de refrigeración más potente si fuera necesario, formado por múltiples ventiladores y que si ocupa una unidad.



Figura 23. Ventilador para refrigeración superior del rack (No ocupa unidad)

En las figuras 5.2.1 se puede la distribución de la electrónica de red dentro del armario. En el caso del armario de la planta baja las unidades 10 y 11 estarían ocupadas por el modem-router, en el caso del armario de las plantas superiores quedarían libres esas dos unidades.

#U	Elemento	Descripción
1	VACIO	Libre para un posible kit de refrigeración
2	VACIO	Libre para futuras ampliaciones y para mejorar la ventilacion









3		Patch-panel de 48 bocas para puntos de red conmutados
4		
5		Pasa hilos
6		Switch de 48 bocas
7	VACIO	Libre para futuras ampliaciones y para mejorar la ventilacion
8		Patch-panel de 48 bocas para puntos de red conmutados
9		
10		Pasa hilos
11		Switch de 48 bocas
12		Bandeja para colocar el modem-Router (Solo planta baja)
13		
14	VACIO	Libre para futuras ampliaciones y para mejorar la ventilacion
15		Regleta PDU 8 tomas con interruptor

Tabla 5. Representación del Rack

5.3 Direccionamiento lógico de la red

Debido al entorno donde se implantará la solución y al nivel de seguridad requerido, se optará por una red de clase C para 254 equipos como máximo.

Se optará por la red privada 192.168.0.0/24 para la implantación. La dirección de broadcast será 192.168.0.255/24 y la puerta de enlace será el router de salida a Internet, en la dirección IP 192.168.0.1/24. Las direcciones 192.168.0.2/24 a 192.168.0.20/24 estarán reservadas para impresoras, electrónica de red, APs del enlace wifi, etc. El propio modem-router de salida a Internet hará las funciones de servidor DHCP para mayor facilidad y mantenimiento de los equipos conectados.

El servidor DHCP asignará direcciones desde la 192.168.0.21/24 hasta la 192.168.0.254/24, en total 233 direcciones, más que suficientes para los equipos y dispositivos que se prevén conectar inicialmente.

La salida a Internet se realizará a través de una sola dirección IP pública facilitada por el proveedor de acceso contratado en las condiciones pactadas con él (IP fija o dinámica) y se hará NAT a través del módem-router de salida, de ese modo, todo el direccionamiento de la red es privado y no es alcanzable desde Internet directamente.

La mayoría de los equipos a conectar a la red son PCs que tomarán los datos de red (dirección IP, puerta de enlace, servidores de DNS, etc) de un servidor de DHCP, por lo que cualquier cambio en el direccionamiento IP de la red será muy sencillo de implantar porque afectará a pocos elementos: conmutadores, modem-router e impresoras fundamentalmente, que tendrán su IP establecida de forma fija y manual.

Se trata de un centro educativo y no hay datos sensibles en casi ningún equipo conectado a dicha red, salvo quizás en el despacho de dirección y en secretaría. En los equipos con datos sensibles, se puede instalar un Firewall software y no dejar recursos compartidos, con esto será más que suficiente por el momento.

No hay previsiones de crecimiento a corto plazo, por lo que unas 30 direcciones IP más que los puntos de red disponibles, son en principio suficientes para posibles ampliaciones: más equipos, posibles APs de una red wifi entre edificios, etc...

Se prevé la instalación de 132 PCs en total en la fase inicial contemplada en este proyecto, con la posibilidad de ampliar hasta los 200 aproximadamente según los puntos de red disponibles que se encuentran conectados a un switch. En una segunda fase de ampliación si fuese necesaria, se podría llegar a 66 equipos más, pero esto requería por un lado la conmutación de los puntos de red desplegados que en esta fase y que no van a ser conectados a un switch, y por otro lado la redefinición lógica de la red, ya que llegados a ese punto, una red de clase C no sería suficiente para direccionar todos los equipos disponibles (más de 254).

5.4 Elección del cableado y velocidad de la red

Basándonos en el mercado actual y la electrónica de red del tipo Gigabit Ethernet, queda claro que se impone ante el resto de opciones disponibles, ya que por muy poca diferencia en la inversión inicial, se obtiene mucha más rentabilidad en lo que a efectividad, velocidad, calidad, escalabilidad y potencial de la red se refiere.

Una vez elegido el estándar Gigabit Ethernet para el despliegue de la red, es importante definir desde el principio el tipo de cableado a usar en la red a desplegar y sus características. En este caso se optará por un cable de cobre tipo UTP rígido y libre de halógenos. Siempre es interesante que el cable esté libre de halógenos, pero en este caso, lo es más, ya que se trata de una instalación donde hay muchos niños y es muy importante minimizar cualquier riesgo, en este caso, de incendio. Además el coste de implantar una solución libre de halógenos no será especialmente representativo, puesto que, a pesar de ser algo más caro, la inversión se realiza una sola vez.

La norma IEEE 802.3ab, ratificada en 1999, define el funcionamiento de Gigabit Ethernet sobre cable de cobre UTP de categorías 5, 5e y 6. Se pueden

encontrar muchos argumentos a favor y en contra sobre si se debe utilizar categoría 5 / 5e ó 6 para implantar Gigabit Ethernet. En este caso se optará por un cable de categoría 6 porque actualmente la diferencia de precio entre ambas posibilidades no es muy importante, la inversión se realiza sólo al principio y merece la pena que la instalación esté lo más preparada posible para abordar ampliaciones futuras y maximizar su durabilidad en el tiempo.

Desde el punto de vista técnico la diferencia general entre las categorías 5e y 6 es la eficiencia en la transmisión. Mientras que 5e tiene un ancho de banda de 100 MHz por par, la categoría 6 llega a los 200 MHz por par. Esto redundará en una mejor relación señal/ruido, ofreciendo mayor fiabilidad y mayores velocidades de transmisión para futuras aplicaciones. Por otro lado, la categoría 6 es la más ampliamente recomendada por los fabricantes de electrónica de red para el despliegue de redes Gigabit Ethernet.

5.5 Elección y configuración de la electrónica de red

5.5.1 Switches y su configuración

Se han barajado varias posibilidades para los Switches, sin perder de vista la idea general de conseguir un equilibrio entre calidad y precio, se pensó en varios modelos, todos ellos son modelos gestionables en todas sus bocas, pero finalmente nos hemos decidido por el DES-1210-52, 48-port 10/100Mbps Fast Ethernet Smart Switch de D-Link (figura 5.5.1). Gestionable e instalable en Rack de 19" de 48 puertos, el DES-1210-52 forma parte de los switches Web Smart de tercera generación de D-Link, que integran avanzadas funciones de gestión y seguridad que garantizan el rendimiento y la escalabilidad.

Este switch es fácil de usar y, al mismo tiempo, una completa y asequible solución para las pequeñas y medianas empresas. Dispone de un innovador diseño sin ventilador y carcasa metálica de 19".

Todos los puertos admiten autonegociación de MDI/MDIX crossover, con lo que los cables crossover o los puertos uplink resultan innecesarios y la conectividad hasta el punto de trabajo es más sencilla y económica. A 2000

Mbps full duplex, los uplinks Gigabit ofrecen canales de datos de alta velocidad a la troncal con una mínima pérdida de datos en la transferencia.

La innovadora función Safeguard Engine de D-Link protege el switch contra el flujo del tráfico generado por los ataques de virus. Por otra parte, el switch soporta las listas de control de acceso (ACL) y la autenticación basada en el puerto 802.1X a través de servidores RADIUS externos, que en este caso no los hay. La vinculación IP-MAC-puerto permite a los administradores seguir la localización de las direcciones IP vinculando la IP de origen con la dirección MAC y el puerto de origen asociados.

Para mayor seguridad, la función1 de rastreo del servidor DHCP controla los paquetes de servidores DHCP maliciosos desde los puertos de los usuarios para evitar la asignación no autorizada de direcciones IP.

El control de ancho de banda permite que el administrador de la red pueda reservar ancho de banda para aquellas importantes funciones que requieren más ancho de banda o una mayor prioridad.

Como características de mantenimiento de la red cuenta con detección de bucles de retorno y diagnóstico de cable. La detección de bucles de retorno se utiliza para detectar bucles creados por un determinado puerto y apagar automáticamente el puerto afectado. El diagnóstico de cable permite a los administradores de red examinar rápidamente la calidad de los cables de cobre, así como determinar el tipo de error que presenta el cable.

Esta tercera generación de switches Web Smart ofrece una gestión fácil y sencilla de la red a través de la intuitiva utilidad SmartConsole y de la interfaz de gestión basada en web. La utilidad SmartConsole permite que los administradores identifiquen fácilmente los distintos switches Web Smart que se encuentren dentro del mismo segmento de red de nivel 2: los switch se muestran en la pantalla para poder acceder a ellos al momento. Con esta utilidad, los usuarios no han de cambiar la dirección IP de su PC. Por otra parte, facilita la configuración inicial de los switches Smart.

Todo ello permite realizar una amplia configuración de los parámetros del switch y una básica configuración de los dispositivos detectados, como, por ejemplos, cambios de las contraseñas y actualizaciones del firmware.

Estos equipos incluso son capaces de distinguir el tráfico de audio (VoIP), y separarlo en otra VLAN y así darle mayor calidad. Pero todo esto sería para posibles mejoras en un futuro.

Puesto que en principio no se van a implementar VLANs ni se van a unir puertos haciendo trunk, la configuración de fábrica que viene con los switches será suficiente, sólo habrá que seguir el manual de usuario para cambiar su dirección IP, el nombre de usuario y la contraseña de administración.



Figura 24. D-Link DES-1210-52

Característica	Valor
Puertos LAN	48
Tipo y velocidad puertos LAN	RJ-45 10/100 Mbps
Puertos uplink fibra ópticos	2
Puertos uplink RJ45 10/100/1000	2
Puertos utilizables simultáneamente	52
Gestión	SmartManaged
VLAN soporte	256
Tabla MAC	8000

Modalidad de Stacking	Virtual
Quality of Service (QOS)	Si
Dimensiones	44X250X440 mm
Peso	3300 gr.
Led	Power, Actividad, Link, Velocidad
Certificaciones CEE	FCC Class A, CE Class A, IC Class A, VCCI Class A, C-Tick

Tabla 6. Características básicas del Switch D-1210-52

5.5.2 Puntos de Acceso

Existe la necesidad de tener un enlace wifi en modo WDS en el centro lo que dará una velocidad suficiente al servicio.

La primera decisión que debemos tomar es el tipo de tecnología Wifi a utilizar, nosotros optaremos por el estándar 802.11ac, ya está totalmente aprobado por el IEEE en el 2014. El estándar consiste en mejorar las tasas de transferencia hasta 433 Mbit/s por flujo de datos, consiguiendo teóricamente tasas de 1.3 Gbit/s empleando 3 antenas. Opera dentro de la banda de 5 GHz, amplía el ancho de banda hasta 160 MHz (40 MHz en las redes 802.11n), utiliza hasta 8 flujos MIMO e incluye modulación de alta densidad (256 QAM).

Una vez decidido este estándar, la banda donde trabajaremos será la de 5Ghz., es una banda menos congestionada, con menos interferencias ya que no hay otras tecnologías que la estén utilizando lo que dará más claridad a la señal.

La siguiente decisión a tomar es que tipo de AP's vamos a utilizar, nosotros nos hemos decidido por el modelo Cisco MR34 por sus excelentes prestaciones y perfecto para cualquier mejora que se quiera hacer.



Figura 25. AP Cisco MR32

Este equipo cumple con el estándar 802.11ac y puede funcionar en modo WDS. En este caso se ha optado por un sistema WDS con posibilidad de admitir clientes, por lo cual el cifrado será AES basada en hardware.



Figura 26. Enlace WDS con admisión de clientes

Al enchufarlo, el punto de acceso MR34 se conecta automáticamente a la nube de Meraki, descarga su configuración y se une a la red correspondiente. A continuación, el MR34 se optimiza automáticamente, determinando el canal, la potencia de transmisión y los parámetros de conexión cliente idóneos. Y si fuera necesario, también dispone de autorrecuperación, respondiendo de forma automática a fallos de conmutadores y otros errores.

Con respecto a la seguridad este dispositivo tiene un sistema WIPS integrado y altamente optimizado realiza una búsqueda continua de amenazas y las soluciona según lo ordenado, todo ello sin que el servicio al cliente se vea afectado.

Características	Valor
Radios (simultaneos)	802.11b/g/n de 2.4Ghz 802.11a/n/ac de 5 Ghz WIPS banda doble y analisis
Interfaces	1 ethernet 100/1000Base-t (RJ-45) Alimentación CC
Seguridad	Firewall integrado Políticas dispositivos móviles WIPS en tiempo real con alarmas Represion de AP no autorizados Aislamiento de visitantes
Cifrado	WEP,WPA,WPA2-PSK,WPA2-Enterprise con 802.1X, TKIP Y AES
Estándares	802.11ac y 802.11n
Dimensiones	253,4 mm x 155,8 mm x 37,1
Peso	700Gr.

Tabla 7. Características AP MR34 de Cisco

Como el MR34 se configura automáticamente y se gestiona a través de Internet, puede implementarse en ubicaciones lejana sin necesidad de tener personal de informática en el sitio.

Para que el sistema funcione correctamente, los AP's deben cumplir las características detalladas en la tabla 5.4.2.5 de forma general.

Parámetro	Configuración
SSID	Puede ser igual en cada AP de la red WDS
Canal	Debe ser igual en todos los AP de la red WDS
Velocidad	Debe ser igual en todos los AP de la red WDS: 802.11a/b/g/n
Modo de trabajo	Cada AP puede funcionar como repetidor o como repetidor y AP aceptando clientes
Cifrado	Todos los AP de la red WDS deben tener el mismo tipo de cifrado y la misma clave

Tabla 8. Datos que deben cumplir los equipos miembros de una red WDS

La distribución de los AP's del edificio, se pueden ver en el Anexo A

5.5.3 Modem-Router de salida a internet

La salida de toda la red hacia internet se realizará a través de una línea de fibra óptica, en cualquier caso se elegirá el operador que mejor oferta tenga en ese momento.

El equipo elegido para gestionar la conexión es el modem router WRT1900AC de Linksys, por sus características es el más adecuado a la red que estamos montando, soporta cualquiera de los modos de conexión más utilizados en nuestro país.

Es un dispositivo que soporta los estándares 802.11b/a/g/n/ac, emite en las bandas de 2.4Ghz y 5 GHz simultáneamente con una velocidad AC1900 (N600+AC1300) tiene una cobertura inalámbrica muy buena gracias a sus cuatro antenas externas lo cual le hace perfecto para un entorno con muchas interferencias.



Figura 27. Modem- Router WRT1900ACS

Características	Valor
Procesador	1.6 Ghz dual-core ARM based
Memoria	128Mb. Flash, 512 DDR3 RAM
Dimensiones	121x75x26 mm
Peso	722.2 Gr
Seguridad	WPA/WPA2/128 bit AES link encryption
Encriptación inalámbrica	64/128-bit WEP/WPA2 personal/WPA2 Enterprise

Tabla 9. Características Modem-Router WRT1900ACS

5.6 Otros elementos de apoyo docente

5.6.1 Equipos y Software básico

Tan importante como la red de conexión entre los equipos son los propios equipos, ya que sin ellos nada tiene sentido, puesto que son el vehículo de acceso a la red y los servicios que esta ofrece. Debido al entorno en el que se utilizarán los equipos, para este proyecto se equiparán con el sistema operativo Microsoft Windows 10 de 64 bits por los siguientes motivos:

- Es un sistema operativo de última generación, lo cual hará que los equipos se amorticen durante más tiempo.

- Microsoft Windows es conocido por casi todo el mundo.
- Las licencias no representan un coste adicional, ya que están incluidas con el equipo.
- La mayoría del software diseñado para la docencia está disponible sólo en plataforma Microsoft.

Una vez decidido el sistema operativo, se instalarán aplicaciones básicas y gratuitas para el mayor aprovechamiento de los equipos, tal como se ve en la tabla 5.6.1.

Aplicación	Descripción
PDF Creator	Impresora virtual que permite convertir a PDF cualquier documento de cualquier programa que sea capaz de imprimir en Microsoft Windows
Adobe Acrobat Reader	Lector de archivos en formato PDF
XNView	Potente gestor de imágenes capaz de manejar más de 45 tipos de formatos, realizar conversiones por lotes, visualizaciones, presentaciones, etc...
Open Office	Suite similar en características a Microsoft Office, pero totalmente gratuita. Incluye un procesador de textos, hoja de cálculo, base de datos, etc...
7Zip	Software de compresión y descompresión de archivos
Mozilla Firefox	Navegador web compatible con HTML 41.0, potente, escalable a través de plug-ins, rápido y eficaz
Codecs de DivX	Formato de vídeo MPG4 para poder visualizar documentación audiovisual

Video LAN	Reproductor multimedia capaz de reproducir DVDs, archivos de sonido y video (según codecs instalados), etc...
Paint .NET	Aplicación gratuita de retoque fotográfico
Maquina Virtual Java	Necesaria para ejecutar multitud de aplicaciones generadas por la administración y otros organismos públicos y privados disponibles en el mundo docente
.NET Framework	Plataforma necesaria para que funcionen las aplicaciones Microsoft de última generación (varias versiones)

Tabla 10. Aplicaciones a instalar en los PC`s del centro

Además de estas aplicaciones, se instalará un sistema de congelación del PC.

Este tipo de sistemas son casi obligados en un entorno como el que nos ocupa, ya que regeneran el PC al estado inicial en cada reinicio (iconos, programas, etc), deshaciendo cualquier cambio intencionado o malintencionado por parte del usuario. Para la implantación de este sistema, el disco duro del equipo tendrá dos particiones, una dedicada al sistema operativo de unos 50Gb, que es la que se congelará y otra con el resto de capacidad del disco dedicada a datos, que no estará congelada y que se destinará a que los usuarios puedan dejar en ella información y que no se pierda entre reinicio y reinicio del PC.

La aplicación elegida para realizar esta función de congelación es de pago, la desarrolla la empresa Faronics y se llama Deep Freeze. Existe alguna solución gratuita como el sistema Steady State de Microsoft, pero no ofrece la versatilidad de Deep Freeze. También hay soluciones por hardware, pero tienen mayor coste y mayor índice de error que una aplicación software. La diferencia fundamental entre Deep Freeze y Steady State es que Deep Freeze funciona por encima del nivel de usuario, por lo que aún siendo administrador

del equipo no se puede desinstalar sin la correspondiente password de administración de su propia consola, mientras que el Steady State se puede manipular si se poseen permisos administrativos a nivel Windows en la máquina.

La instalación es muy sencilla, una vez llegados al punto de correcta instalación y configuración de todas las aplicaciones que estarán disponibles en el PC, basta con ejecutar el instalador de Deep Freeze y elegir que partición queremos congelar, en este caso la del sistema.

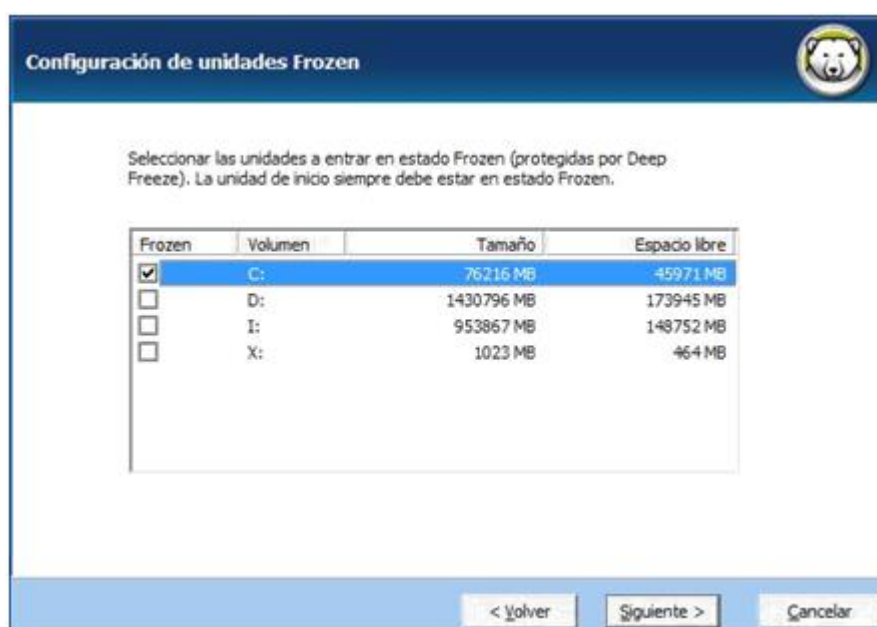


Figura 28. Pantalla de elección de unidades congeladas durante la instalación de Deep Freeze

Una vez instalado, el sistema se reinicia activando la congelación. Se puede apreciar a través de un mini icono en la barra de tareas.



Figura 29. Barra de tareas, icono de estado de Deep Freeze

Cualquier cambio en el equipo solo tendrá efecto hasta que reiniciemos de nuevo, momento en el cual todo volverá al punto en el que se instaló Deep Freeze y el sistema quedó congelado. Si se desea actualizar o instalar alguna aplicación, cambiar el entorno de trabajo, drivers, etc, basta con acceder al panel de administración de Deep Freeze haciendo doble click sobre el icono mientras se pulsa la tecla de mayúsculas e introducir la contraseña.



Figura 30. Ventana de introducción de password en Deep Freeze

Después hay que indicar al sistema que no se desea mantener la congelación en el siguiente reinicio y reiniciar el PC.

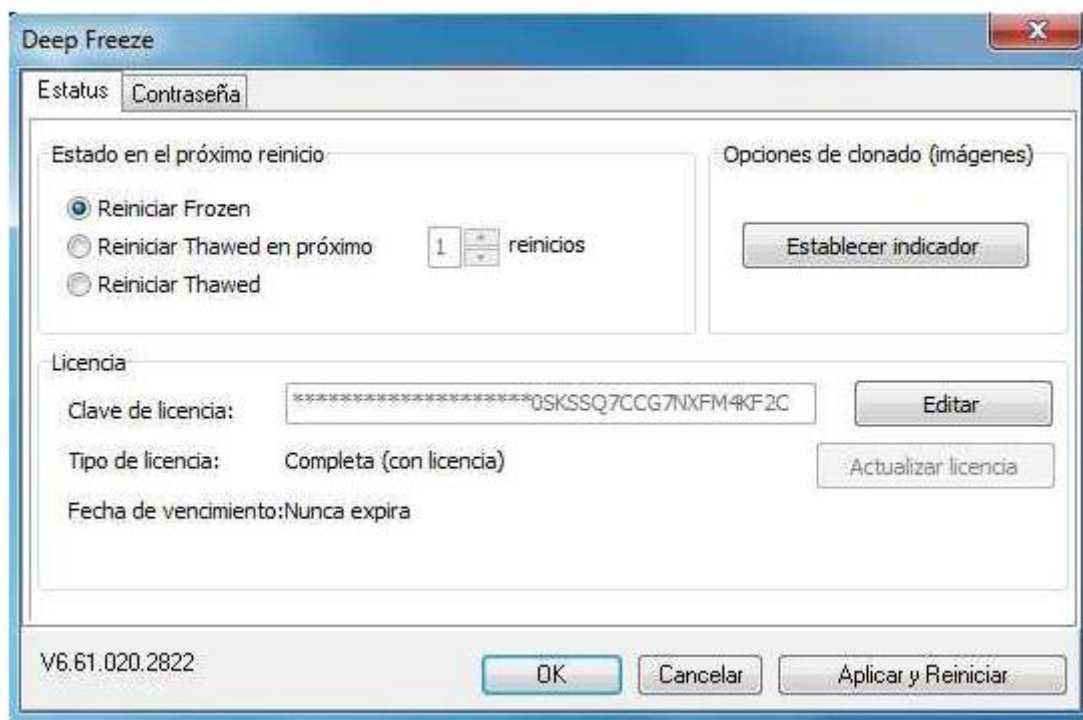


Figura 31. Panel de control de Deep Freeze

A partir de ese momento todos los cambios serán permanentes hasta que se vuelva a activar de nuevo el modo congelado.

También existe un modo alternativo de trabajo rápido, indicando a Deep Freeze que se desea trabajar en modo descongelado los próximos X reinicios de la máquina, de modo que al alcanzar ese número, el modo congelado se activa automáticamente. Esta opción es muy interesante para agilizar la instalación de aplicaciones puntuales en las que se sabe de antemano las veces que se reiniciará el PC para completar el proceso de instalación.

Este tipo de sistemas de congelación es básico para minimizar las averías, ya que en condiciones normales con estos sistemas activos las averías serán sólo físicas por rotura de ratones, teclados, fuentes, placas base, etc, pero un PC nunca dejará de estar operativo porque se han desconfigurado los drivers de la tarjeta de red o video, por un virus, etc. Este escenario minimiza el gasto en servicio técnico y maximiza la productividad y disponibilidad de los equipos, amortizando el coste de las licencias en muy poco tiempo.

Gracias a este sistema, los equipos también están libres de virus permanentemente, por lo que no es necesario a priori instalar un antivirus.

La relación de equipos a instalar en las diferentes aulas y salas viene descrita en la tabla 5.6.1.1 para los edificios de primaria e infantil respectivamente.

EDIFICIO PRINCIPAL	
ESTANCIA	EQUIPOS A INSTALAR
PLANTA BAJA(47)	
Aulas de Infantil (1-10)	10
Aula Polivalente ESO Aula Informática	27
Relaciones Externas	1
Secretaría	1
Administración	1
Dirección	1
Coordinación infantil	1
Tutoría	1
Sala de profesores	4
PLANTA PRIMERA (50)	
Aulas de Primaria (1-12)	12
Despacho Coordinación Primaria	1
Sala de profesores	4
Despacho Coordinador	1
Tutoría	1
Laboratorio ESO	1
Aula Polivalente ESO Aula Informática	27
Biblioteca Primaria y ESO	3
PLANTA SEGUNDA (49)	
Aulas Primaria (13-18)	6

Aulas Polivalentes ESO (1-3)	3
Aula Polivalente ESO (12) Aula Informática	27
Taller Tecnología Bachillerato	1
Sala Profesores	4
Aula Pequeño Grupo EPO(1-6)	6
Taller Polivalente Música, Tecnología, ESO y Primaria	1

Tabla 11. Desglose de equipos a instalar

5.6.2 Impresoras

Las impresoras son un elemento importante y fundamental en la dotación informática de un centro de enseñanza. Debe haber dispositivos con prestaciones suficientes para cubrir las necesidades de la dirección, los docentes, etc.

En todos los casos se usarán dispositivos láser por eficiencia y productividad, se imprimirá mucho y deben ser dispositivos preparados para ello.

Se instalará un dispositivo multifunción láser color con capacidad de fax y escáner para la sala de secretaría, que será usado para labores administrativas y por el despacho de relaciones externas del centro, ya que está al lado.

También se instalarán impresoras láser multifunción con escáner en las salas de profesores a disposición de los docentes y otra más en la administración del centro. Por último la dirección tendrá su propia impresora laser B y N.

Todos los dispositivos dispondrán de tarjeta de red y de opción duplex para imprimir a doble cara de forma automática.

Para este caso se ha diseñado la distribución de impresoras en el centro que se indica en la tabla 12.

Edificio principal		
Estancia	Impresoras	Modelo
Planta baja		
Dirección	1	Aficio SP4310N
Secretaría	1	MPC 4503SP
Administración	1	MPC 4503SP
Sala de profesores	1	MPC 4503SP
Primera Planta		
Sala de profesores	1	MPC 4503SP
Segunda Planta		
Sala de profesores	1	MPC 4503SP

Tabla 12. Desglose de impresoras a instalar

Se ha optado por la marca RICOH frente a otras clásicas por varias razones:

- La oferta es muy clara y es sencillo escoger los modelos apropiados para cada caso y cada necesidad.
- Se ofrecen 3 años de garantía para todos los productos.
- Hay buena relación de precio en las páginas que se imprimen.
- Consumibles gratis, facilidad para pedirlos directamente en su web de soporte.
- Servicio técnico en menos de 24 horas para cualquier avería de las máquinas.

En la tabla 5.6.2.1 se aprecian las características de las impresoras instaladas en cada zona.

MPC 4503SP	
Características	Valor
Velocidad	45 ppm
Peso	100 kg.
Dimensiones	587 x 685 x 963 mm
Memoria	2 Gb.
Funciones	Impresora, fotocopidora, fax, escáner,
Aficio SP4310N	
Características	Valor
Velocidad	36 ppm
Memoria	512 MB.

Tabla 13. Características impresoras

5.6.3 Pizarras digitales y proyectores

Las pizarras digitales son la evolución natural de las clásicas pizarras de tiza. Se puede hacer lo mismo que con ellas: borrar, trazar, escribir, etc, con la gran ventaja de que cada pizarra, una vez escrita se puede almacenar y durante la clase se puede volver a ella si fuese necesario.

El concepto de pizarra digital va inexorablemente unido a un proyector, de hecho se conoce como PDI (Pizarra Digital Interactiva) al conjunto compuesto por un dispositivo señalador, una superficie de proyección y un proyector.

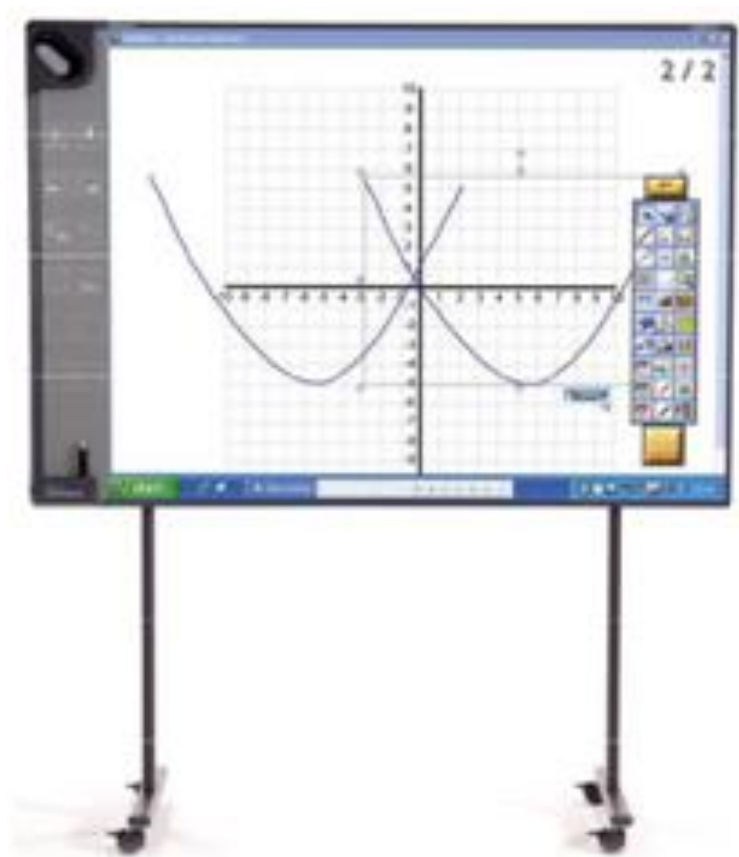


Figura 32. PDI

Para este proyecto se ha elegido el modelo de PDI MCI780 de la empresa Multiclass. Se trata de una pantalla táctil de 78" cuenta con tecnología infrarrojo que permite su utilización hasta 4 usuarios de forma simultánea y reconocimiento de gestos que hacen que su utilización sea aún más fácil. Es de fácil limpieza y con una resistente superficie Cerámica que permite su utilización como pizarra blanca con cualquier tipo de rotulador de borrado en seco (no deja marcas). Al ser táctil puede funcionar sin dispositivo señalador activo específico, tan solo con el dedo o un bolígrafo o rotulador cerrado, puntero de plástico, etc.

En este tipo de pizarras, ya se incluye el proyector para poder reproducir cualquier tipo de archivo multimedia.

La gran ventaja de esta nueva generación de proyectores frente a los clásicos es que están ubicados sobre la cabeza del hablante y por lo tanto no genera sombras porque el hablante no se pone delante de la proyección, que viene desde arriba. Otra gran ventaja es que la instalación de este tipo de

modelos de proyector minimiza la canalización necesaria y la dificultad de llevar el cableado VGA, corriente eléctrica, audio, etc por el techo, siendo más sencillo hacerlo por detrás de la propia pizarra hacia el PC que usa el profesor, ahorrando en metros canalización y cableado de todo tipo, así como mejorando la estética de la instalación.

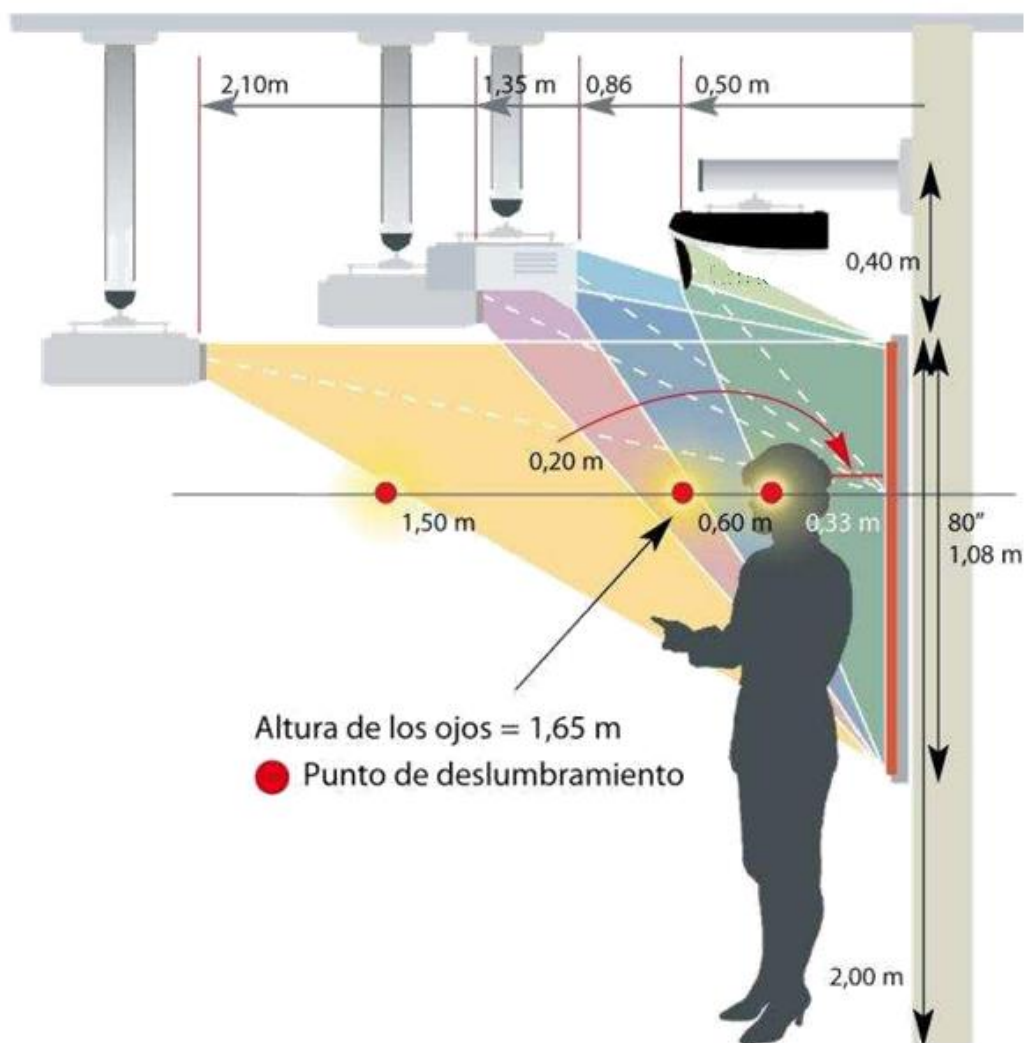


Figura 33. Capacidad de instalación del proyector de corto alcance

6. Presupuesto

A continuación se detalla un presupuesto aproximado para la completa implantación de la solución propuesta. Se han indicado algunos de los proveedores más conocidos del mercado español donde se puede encontrar el material referenciado.

Los precios indicados aquí son orientativos PVP por lo que habría que quitarle entre un 20% y un 30% de media para obtener PVD.

Presupuesto de instalación de la red y electrónica necesaria:

Producto	Proveedor	Precio/unid.	Cantidad	Precio
Rack mural 19" de 15 unidades con puerta de cristal y cerradura en puerta y en lateral (Ref. 24050)	Ingesdata	416,00	3	1.248,00
Kit de ventilación superior para rack sin consumir unidad (Ref. 2542)	Ingesdata	165,00	3	495,00
Patch-panel Cat. 6 48 bocas (Ref. PPC-6-U-48)	Ilumitec	65,50	6	390,00
Pasahilos (Ref. 5526)	Ingesdata	25,00	6	150,00
PDU Regleta eléctrica 12 tomas Schuko	Ingesdata	64,00	3	192,00
Bandeja soporte de 250 mm de fondo (Ref. 2400)	Ingesdata	34,00	1	34,00
Kit de tuerca enjaulada, tornillo y arandela para montaje en rack (Ref. 2352)	Ingesdata	0,62	105	65,10
Latiguillos 150 cm RJ45 Cat.6 para conexión interior en los racks (Ref. 1451)	Ingesdata	3,84	288	1.105,92

Cable UTP Cat. 6 libre de halógenos. Bobina de 305m (Ref. 0115)	Ingesdata	94,00	8	752,00
Rosetas dobles de superficie con salida lateral y conexión RJ45 Cat. 6 (Ref. 1289)	Ingesdata	12,00	106	1.272,00
Canaleta central para pasillos (50x100 m con doble cuerpo, en paquetes de 16 m). Total 180 m (60 m/Planta)	Ingesdata	119,00	12	1.428,00
Canaleta para despliegue en las estancias (16x20 m en paquetes de 140 m). Total 870 m	Ingesdata	128,00	7	896,00
Switch DES-1210-52 D-link	CiudadWireless	295,92	6	1.774,92
AP Cisco Meraki MR34	Amazon	741,15	10	7.411,50
Mano de obra para instalación de HW		5000,00	1	5.000,00
Mano de obra de configuración SW		75,00	15	1.125,00
Total				23.339,44

Tabla 14. Presupuesto electrónica de red

Presupuesto de instalación de las pizarras, los proyectores y los equipos de las aulas, salas de profesores, etc. Esta partida se podría aplicar por fases si el presupuesto resulta alto, dotando a las aulas de equipamiento de forma progresiva a lo largo de varios cursos:

Producto	Proveedor	Precio/unid.	Cantidad	Precio
Pc para las aulas, salas de profesores, etc... - Cpu intel core i3 4170 3.70 ghz - placa base asus h81m-k s1150 matx 2ddr3 sata - 4gb memoria kingston ddr3 pc1600 - 1 disco seagate integracion sata3 500gb 16mb - regrabadora lg dvd-rw interna 24x - grafica integrada - caja matx 500w thyra. Minitorre audio negra - garantia 2 años	Alser-Informática	310,00	146	45.260,00
Licencias Windows 10	Alser-Informática	90,00	146	13.140,00
Monitor asus vb199t 19"	Alser-Informática	139,00	146	20.294,00
Licencias Deep Freeze	Faronics	9,00	146	1.314,00
PDI multiCLASS (Pizarra táctil 78.2"+ curso formación online +proyector+soporte+altavoces+ caja conexiones)	Multiclass	1461,00	43	62.823,00
Impresora RICOH MPC4503	Ricoh	699,00	5	3.495,00
Impresora RICOH Aficio SP4310N	Ricoh	255,00	1	255,00
Material adicional (cables VGA, latiguillos USB,...)		750,00	1	750,00
Total				147.331,00

Tabla 15. Presupuesto equipamiento informático

7. Posibles mejoras y perspectivas de futuro

Son múltiples las posibles mejoras que se pueden hacer en esta instalación. De hecho, durante el desarrollo del proyecto se han indicado algunas de ellas sobre la marcha. En este caso, al tratarse de un entorno docente, con un presupuesto ajustado, no se han tenido en cuenta algunos aspectos básicos en un entorno empresarial, como cortafuegos, zonas D.M.Z. para servidores, VLANs, etc.

Algunas mejoras que se pueden hacer en ese aspecto en esta instalación son las siguientes:

- Equipos dedicados a los alumnos: Durante este proyecto solo se han puesto equipos para los alumnos en las aulas informáticas, sería una mejora no muy costosa y que daría un plus de ayuda a la docencia colocar un par de PC's en cada aula para búsqueda de información de los alumnos.
- Servidor: Se podría poner un servidor RADIUS para autenticación de cada profesor e incluso poner algún usuario genérico para alumnos o para aulas. De esta manera la seguridad sería mayor y desde ningún equipo accesible por alumnos se podría acceder a ninguno de profesores o que desde ningún equipo del centro se pueda acceder a modificar los parámetros de la electrónica de red, asignando esa función a un eventual administrador del sistema, etc. Con este mismo servidor se podrían crear políticas de filtrado de internet para que los alumnos no pudieran acceder a material al que no deberían acceder. En nuestro modelo eso es difícil ya que los alumnos solo usarían el PC con un profesor presente durante el transcurso de una clase.
- Enlace WIFI externo: existe la posibilidad de la ampliación del centro con otro edificio. Dicho edificio también deberá disponer de una red informática. Para ello en vez de crear otra red completa, se podría poner dos AP's externos que no admitiesen clientes ya que solo se dedicarían a mantener el enlace wifi y con un armario rack en el nuevo edificio sería suficiente para tener todo en una misma red y con un mismo direccionamiento lógico.

- Trunk: En la implantación propuesta, la troncal que une todos los switches de las plantas está montada sobre un solo cable UTP a Gigabit Ethernet. Una ampliación interesante si se desea mejorar la capacidad de la troncal es ampliar ese enlace entre switches a través de Trunking. Los switches se han elegido estratégicamente para soportar también esa función, de modo que se puedan unir varias bocas físicas del switch en una sola boca virtual consiguiendo la suma de ancho de banda resultante. Es decir, que si se unen 2 bocas, se consigue un enlace a 2 Gbps, si se usan 4 el enlace será 4 Gbps, etc. Técnicamente según la documentación del switch se podrían hacer trunking hasta con 12 puertos, lo que nos daría 12 Gbps de ancho de banda entre switches. Realmente, con 4 Gbps sería más que suficiente si algún día se quisiera implantar esta mejora. Para ello habría que crear una troncal paralela con tantos cables UTP como Gbps queramos aumentar y conectarlos en las bocas 47 y anteriores de los correspondientes switches, siguiendo el esquema propuesto en capítulos anteriores. En todos los switches se ha dejado capacidad suficiente para poder llegar a un trunk de 4 Gbps sin tener que tocar nada más que la aplicación de cable por la canaleta ya existente. Una vez conectados las nuevas bocas de los switches, habría que entrar en el panel de administración de cada uno de ellos e indicar que bocas forman el trunk, sino se producirían problemas y colisiones en la red por haber ciclos entre los switches.

8. Bibliografía

1. Seguridad y fiabilidad en WIFI:
https://es.wikipedia.org/wiki/Wifi#Seguridad_y_fiabilidad
Última Visita: 05/10/2015
2. Cifrado WEP:
https://es.wikipedia.org/wiki/Wired_Equivalent_Privacy
Última Visita: 06/10/2015
3. Arquitectura de redes:
<http://es.slideshare.net/wsar85/arquitectura-de-redes-8321826>
Última Visita: 05/10/2015
4. Modelo OSI, TCP/IP y Estándares:
<http://es.slideshare.net/riveroloja/tema-2-arquitectura-de-redes?related=1>
Última Visita: 05/10/2015
5. Tipos y Características de Cables de red:
<http://es.slideshare.net/QUITUS94/tipos-de-cable-para-una-red-13826211>
Última Visita: 05/10/2015
6. Cifrado WPA:
https://es.wikipedia.org/wiki/Wi-Fi_Protected_Access
Última Visita: 06/10/2015
7. Protocolo IPsec:
<https://es.wikipedia.org/wiki/IPsec>
Última Visita: 06/10/2015
8. Modem-router y especificaciones:
<http://www.linksys.com/es/p/P-WRT1900ACS/#product-features>
Última Visita: 12/10/2015
9. Access Point y especificaciones:
https://meraki.cisco.com/lib/pdf/meraki_datasheet_MR34_es.pdf
Última Visita: 12/10/2015
10. Página oficial de Ricoh:
<http://www.ricoh.es/index.aspx>
Última Visita: 12/10/2015
11. Características Ricoh Aficio SP4310N:

http://www.ricoh.cl/products/product_details.aspx?cid=104&scid=118&pid=2210

Última Visita: 12/10/2015

12. Características Pizarra Digital Interactiva:

<http://www.multiclass.com/educacion/pizarra-digital-interactiva-multiclass-board>

Última Visita: 12/10/2015

13. Proveedor Patch-Panel:

<http://www.ilumitec.es/patch-panel-ppc-6-u.html>

Última Visita: 13/10/2015

14. Página oficial Ingesdata:

<http://www.ingesdata.com/>

Última Visita: 13/10/2015

15. Proveedor ciudadwireless:

<http://www.ciudadwireless.com/>

Última Visita: 13/10/2015

16. Glosario

<i>HW</i>	Hardware.
<i>SW</i>	Software.
<i>PAN</i>	Personal Area Network / Red de Área Personal.
<i>LAN</i>	Local Area Network / Red de Área Local.
<i>MAN</i>	Metropolitan Area Network / Red de Área Metropolitana.
<i>WAN</i>	Wide Area Network / Red de Área Amplia.
<i>WLAN</i>	Wireless Local Area Network / Red de Área Local Inalámbrica.
<i>BBDD</i>	Bases de Datos.
<i>SRA</i>	Arquitectura de Sistemas de Red.
<i>DRA</i>	Arquitectura de Red Digital.
<i>DECnet</i>	Digital Equipment Corporation.
<i>OSI</i>	Open System Interconnection.
<i>PMCD</i>	Protocolo de mensaje para comunicación de datos.
<i>CBS</i>	Comunicación Binaria Síncrona.
<i>ARCNET</i>	Attached Resource Computer NETwork.
<i>IEEE</i>	Institute of Electrical and Electronics Engineers / Instituto de Ingeniería Eléctrica y Electrónica.
<i>CSMA/CD</i>	Carrier Sense Multiple Access with Collision Detection / acceso múltiple con escucha de portadora y detección de colisiones.
<i>PC</i>	Personal Computer / Ordenador Personal.
<i>Gbps</i>	Gigabits por segundo.
<i>MAC</i>	media access control / Control de acceso al medio.
<i>FCS</i>	Frame Check Sequence / Secuencia de Verificación de Trama.
<i>CRC</i>	cyclic redundancy check / Verificación de redundancia cíclica.
<i>IP</i>	Internet Protocol / Protocolo de internet.
<i>ISO</i>	International Organization for Standardization / Organización Internacional de Normalización.
<i>UIT-T</i>	Unión Internacional de Telecomunicaciones.

<i>SO</i>	Operative System / Sistema Operativo.
<i>TCP/IP</i>	Transmission Control Protocol/Internet Protocol / Protocolo de control de transmisión/Protocolo de Internet.
<i>DoD</i>	Department of Defense / Departamento de Defensa.
<i>Telnet</i>	Telecommunication Network.
<i>FTP</i>	Foiled twisted pair / par trenzado con blindaje global.
<i>HTTP</i>	Hypertext Transfer Protocol / protocolo de transferencia de hipertexto.
<i>Bps</i>	Bits Por Segundo.
<i>Kbps</i>	KiloBits por segundo.
<i>Mbps</i>	MegaBits por segundo.
<i>UTP</i>	Unshielded twisted pair / par trenzado sin blindaje.
<i>STP</i>	Shielded twisted pair / par trenzado blindado.
<i>VER</i>	basic encoding rules / reglas básicas de codificación.
<i>WAP</i>	Wireless Application Protocol / protocolo de aplicaciones inalámbricas.
<i>AP</i>	Access Point / Punto de Acceso.
<i>NOS</i>	Network Operating System / Sistema Operativo de Red.
<i>WIFI</i>	wireless fidelity / Fidelidad inalámbrica.
<i>OFMD</i>	Orthogonal Frequency Division Multiplexing / Multiplexación por División de Frecuencias Ortogonales.
<i>MIMO</i>	Multiple input, multiple output.
<i>SSID</i>	Service Set Identifier / nombre de la red.
<i>DHCP</i>	Dynamic Host Configuration Protocol / protocolo de configuración dinámica de host.
<i>WEP</i>	Wired Equivalent Privacy / Privacidad Equivalente a Cableado.
<i>WAP</i>	Wireless Application Protocol / protocolo de aplicaciones inalámbricas.
<i>QSS</i>	Configuración de seguridad rápida.
<i>WPA</i>	Wi-Fi Protected Access / Acceso Wi-Fi protegido.
<i>AES</i>	Advanced Encryption Standard / Estándar de encriptación avanzado.

<i>DES</i>	Data Encryption Standard / Estándar de encriptación de datos.
<i>IPSEC</i>	Internet Protocol security / Protocolo de seguridad de internet.
<i>AH</i>	Authentication Header.
<i>ESP</i>	Encapsulating Security Payload.
<i>IKE</i>	Internet Key Exchange.
<i>NBS</i>	National Bureau of Standards / Oficina Nacional de Normalización.
<i>NIST</i>	National Institute of Standards and Technology / Instituto Nacional de tecnología y estándares.
<i>PDI</i>	Pizarra Digital Interactiva.
<i>NAT</i>	Network Address Translation / Traducción de direcciones de red.
<i>ACL</i>	Access control list / lista de control de acceso.
<i>VoIP</i>	Voz IP.
<i>WDS</i>	Wireless Distribution System / sistema de distribución inalámbrico.
<i>VGA</i>	Video Graphics Array / Adaptador Gráfico de Video.
<i>PVP</i>	Precio de Venta al Público.
<i>PVD</i>	Precio de Venta a Distribuidor.
<i>DMZ</i>	Demilitarized zone / Zona Desmilitarizada.
<i>USB</i>	Universal Serial Bus / Bus Universal en Serie.
<i>RADIUS</i>	Remote Authentication Dial-In User Service.

17. Anexos

10.1 Anexo A – Planos del edificio

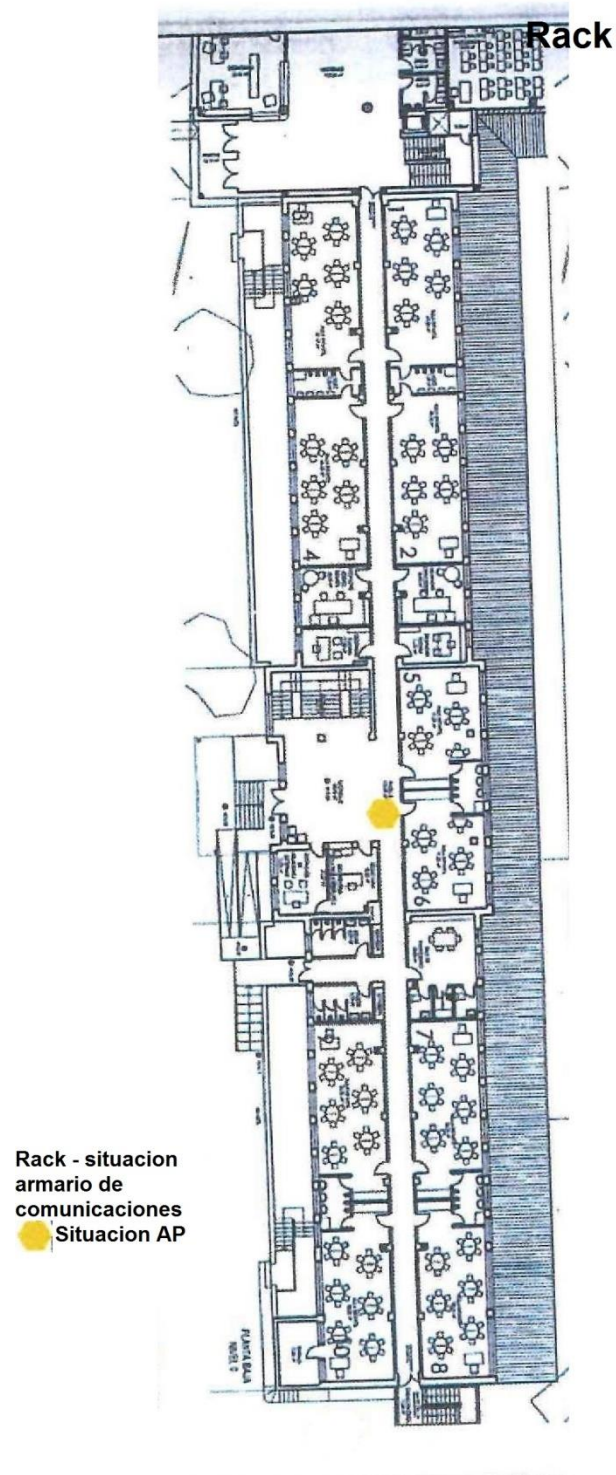


Figura 34. Planta 0 Infantil

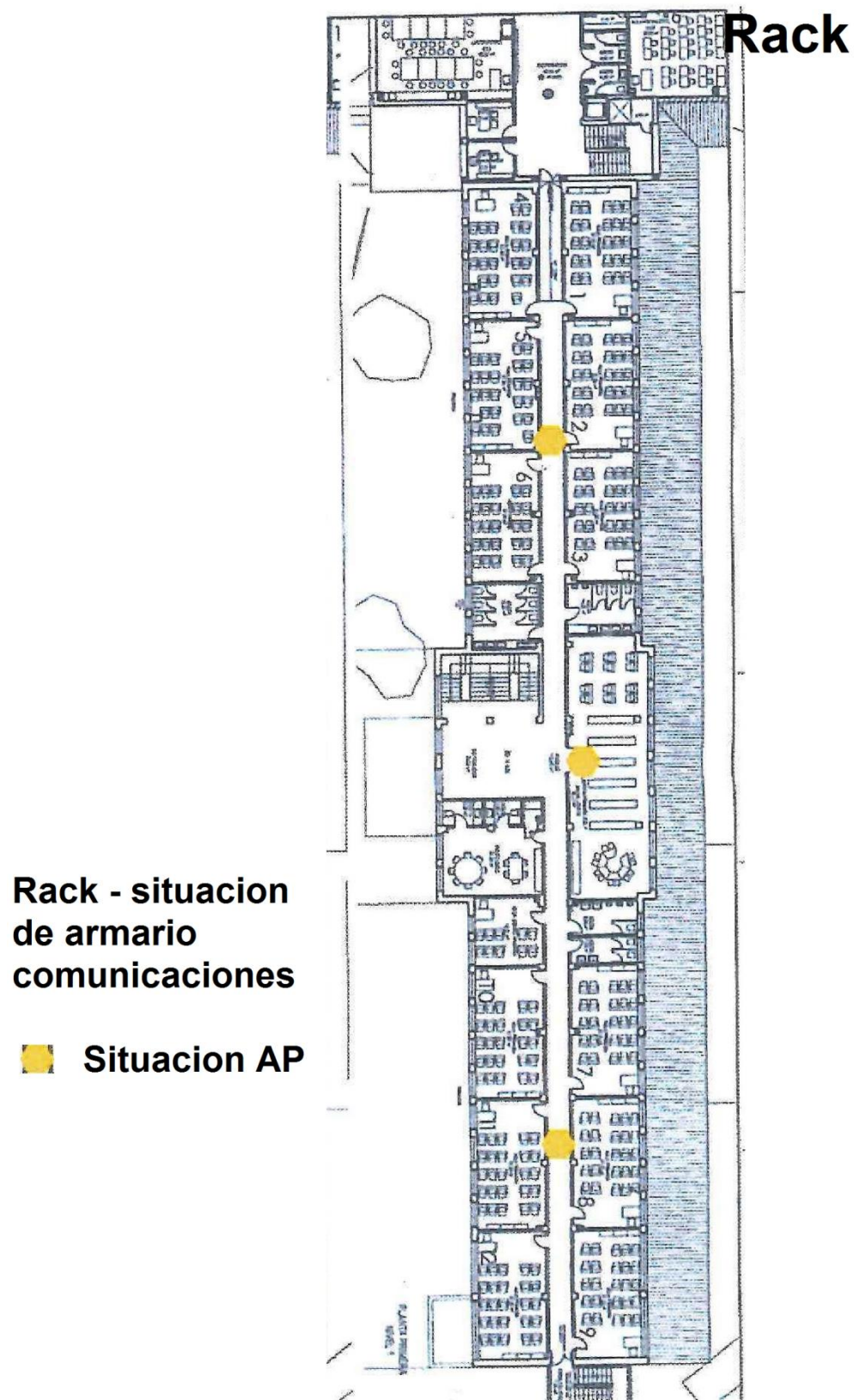


Figura 35. Planta 1 Primaria

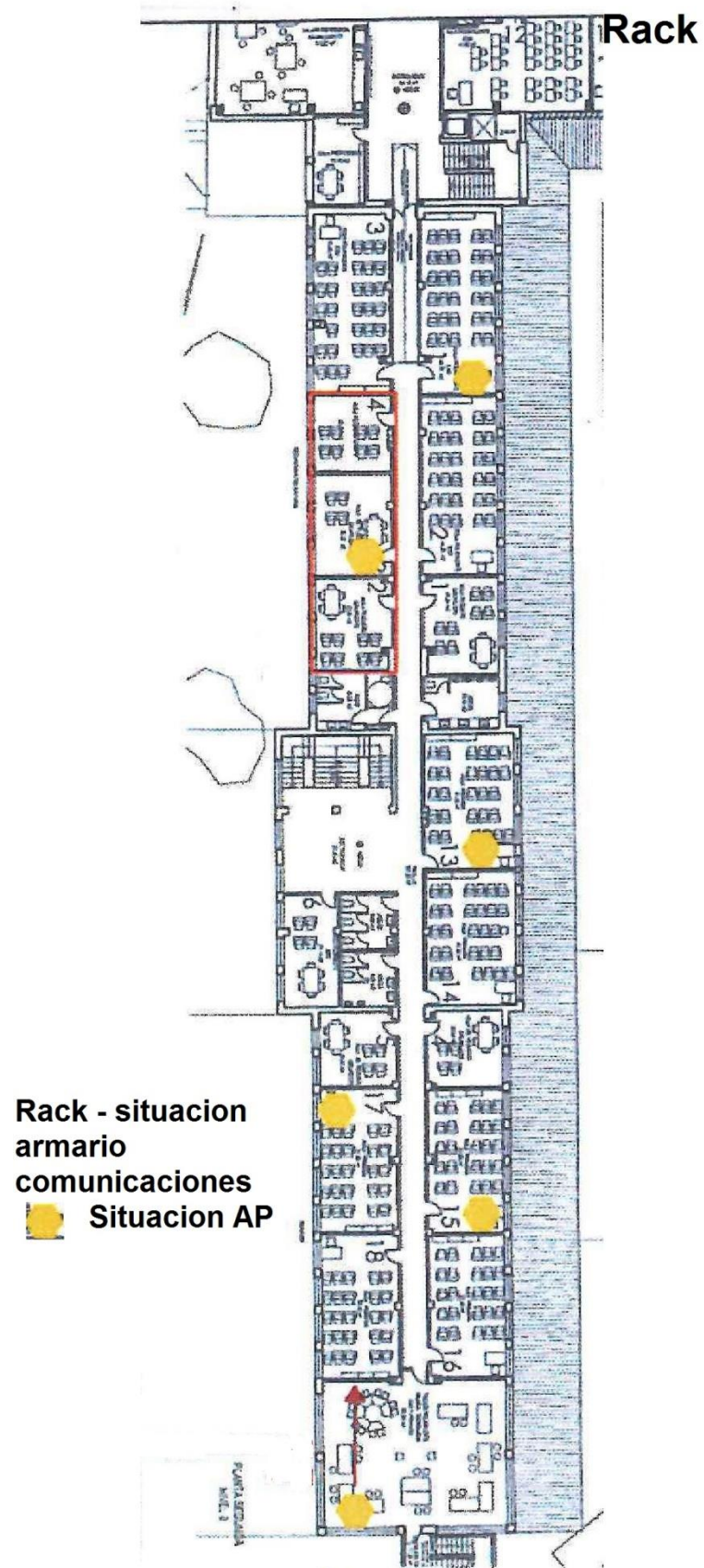


Figura 36. Planta 2 ESO

10.2 ANEXO B - DIAGRAMAS DE RED

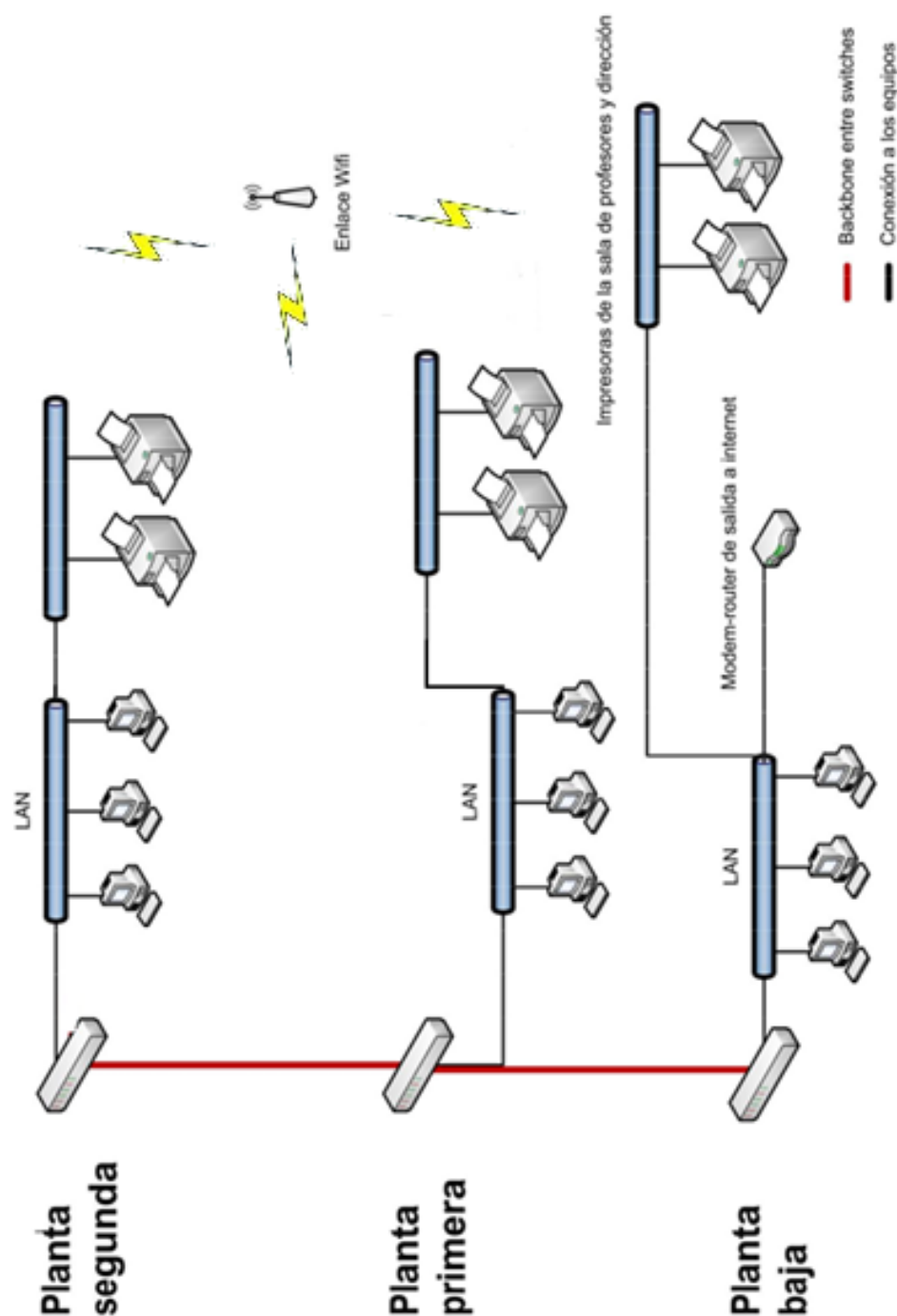


Figura 37. Distribución general de la red